Timo Ingalsuo ja Pasi Paunu (toim.)

Kyberturvallisuus, hyökkäys ja puolustus

INFORMAATIOTIETEIDEN YKSIKKÖ
TAMPEREEN YLIOPISTO

INFORMAATIOTIETEIDEN YKSIKÖN RAPORTTEJA 15/2012

TAMPERE 2012

TAMPEREEN YLIOPISTO
INFORMAATIOTIETEIDEN YKSIKKÖ
INFORMAATIOTIETEIDEN YKSIKÖN RAPORTTEJA 15/2012
MARRASKUU 2012

Timo Ingalsuo ja Pasi Paunu (toim.)

Kyberturvallisuus, hyökkäys ja puolustus

INFORMAATIOTIETEIDEN YKSIKKÖ
33014 TAMPEREEN YLIOPISTO

ISBN 978-951-44-8994-5

ISSN-L 1799-8158
ISSN 1799-8158

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

SEMINAARI

Kyberturvallisuus, hyökkäys ja puolustus

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

08:30 rekisteröityminen
09:00 Marko Mäkipää PITKY ry. : ***Seminaarin avaus*** Pinni B 1096

09:15 Keynote: Jarno Limnéll / director of cyber security, ST / Stonesoft
Strateginen näkökulma kyberturvallisuuteen – kehityssuunta on huolestuttava

10:00 Juha Högmander / project manager,GSEC / Insta DefSec
iKyber: Kyberturvallisuuden johtamisjärjestelmä

10:30 *Kahvitauko*

10:50 Jani Kenttälä Clarified Networks
Miten Suomeen saatiin maailman puhtaimmat verkot

11:20 Jussi / blue team 5 / Baltic Cyber Shield 2010
Taktiikoita, tekniikoita ja menettelytapoja baltic cyber shield 2010 - cdx voittaneelta blue team 5:lta

11:50 *Lounas*

13:00 Keynote: Martti Lehto / tutkija, ST / Jyväskylän yliopisto Pinni B 1100
Kyberturvallisuus ja informaatioturvallisuuden koulutus

	Track 1 Pinni B 1096	Track 2 Pinni B 1100
13:45	Petteri Weckström JAMK ***JYVSECTEC - turvallisuusteknologian kehittämishanke***	Anssi Kärkkäinen PEJOJÄOS ***Cognitive networks and cyber threats***
14:15	Anna-Riitta Leppänen POLAMK ***Tietoverkkorikollisuus –haaste poliisille ja yhteiskuntatieteelliselle tutkimukselle***	Mikael Storsjö Kavkaz-Center ***Suojautumisen ja ennalta varautumisen keinot***
14:45	*Kahvitauko*	
15:05	~~Harry Piela SPSS Finland Oy~~ ~~***Pilvipalveluiden stardardointi ja turvallisuus***~~ ***PERUTTU***	Vesa Keinänen Insta DefSec ***SIEM ja Kybertilannekuva***
15:35	Aleksi Suhonen / BaseN / Trex.fi ***IP-verkkojen luotettavuudesta***	Mikko Jakonen ***Ubiquitous model for managing role based identities and encryption capabilities within cyberspace (including clouds)***

16:05 **Paneelikeskustelu:** Ajatuksia kyberturvallisuudesta. Millaista tutkimusta, koulutusta ja projekteja aiheen ympärille pitäisi rakentaa?
Martti Lehto (JyU) Jari Rantapelkonen MPKK, Sirpa Virta TaY, Ville Viita MPKK, Aleksi Suhonen Trex.fi ja Jani Kenttälä Clarified Networks

16:50 Seminaarin loppupuheenvuoro Pinni B 1029
17:00 Verkostoitumistilaisuus, pikkusuolaista
18:30 adjourn

Lehdistötiedote 28. Elokuuta 2012

Kyberturvallisuudella, eli digitaalisen maailman turvallisuudella, on merkittävin turvallisuusymmärrystä muuttava vaikutus seuraavien vuosien aikana. Tämä koskee niin valtioita, yrityksiä kuin meitä jokaista. Kybermaailmaan liittyvä turvallisuus onkin viimeaikoina noussut useasti julkisuudessa käytävään keskusteluun.

Stonesoft Oyj:n kyberturvallisuusjohtaja tohtori Jarno Limnéll näkee että kansainvälinen valtioiden välinen kyberaseiden varustelukilpailu on käynnissä ja useissa maissa kyberuhkat ovat turvallisuuspoliittisissa arvoissa nousseet vakavimmiksi uhkiksi. Kansainväliset säännöt jotka säätelisivät kybertodellisuudessa tapahtuvia asioita kuitenkin puuttuvat ja nykytilanteen kehityksen voi nähdä hyvin huolestuttavana.

Oleellisimmat muutokset kybertoimintaympäristössä voidaan Limnéllin mukaan tiivistää kolmeen kohtaan: ”Toiminnasta on tullut valtiollista. Resurssointi kyberturvallisuuteen on oleellisesti lisääntynyt ja hyökkäys- ja puolustuskyvykkyyksiä rakennetaan systemaattisesti. Lisäksi yhteiskunnat ovat tulleet tietoisemmiksi haavoittuvuudesta tietoyhteiskuntana”.

Limnéll pitää kybervakoilua ja -rikollisuutta todella vakavina kansainvälisinä ongelmina, joihin yhteiskunnat ei osaa suhtautua vielä riittävällä vakavuudella. ”Suomelle kyberturvallisuus on loistava mahdollisuus, niin poliittisesti, taloudellisesti kuin turvallisuuspoliittisesti. Suomesta löytyy runsaasti korkeatasoista teknistä osaamista, jota tulee kuitenkin merkittävästi lisätä (ja panostaa) lähivuosina. Tämä tarkoittaa muun muassa alan houkuttelevuuden lisäämistä nuorten ja vanhempienkin keskuudessa. Suomesta on mahdollista tehdä maailman johtavia valtioita kyberturvallisuudessa”.

Tampereen yliopiston Informaatiotieteiden yksikkö yhdessä Pirkanmaan tietojenkäsittely-yhdistys PITKY ry:n kanssa järjestää 6.9.2012 yliopiston tiloissa seminaarin aiheesta ”Kyberturvallisuus, hyökkäys ja puolustus”. Jarno Limnéll pitää alan pitkäaikaisen vaikuttajan sotatieteen tohtori Martti Lehdon kanssa seminaarin pääpuheenvuorot. Limnéll puhuu aiheesta ”strateginen näkökulma kyberturvallisuuteen”, ja Lehdon teemana on kyberturvallisuus ja informaatioturvallisuuden koulutus.

Seminaarin tarkoituksena on kerätä yhteen suomalaisia turvallisuusalan toimijoita, sekä tutkimuslaitoksien että yrityksien edustajia, kertomaan, kuulemaan ja keskustelemaan kyberturvallisuuden ajankohtaisista asioista ja uusimmista kehityssuuntauksista sekä verkostoitumaan yhteistyön merkeissä. Teemallisesti seminaarin aiheissa painotetaan kyberturvallisuuden käytäntöjä ja teoriaa sekä näiden uusinta kehitystä.

Lisätietoja seminaarista antaa erikoistutkija Marko Mäkipää, 0504280882

Kyberturvallisuusseminaari – seminaarin avaus 6. Syyskuuta 2012

Marko Mäkipää, erikoistutkija, Tampereen yliopisto ja PITKY ry

Hyvät naiset ja herrat, hyvää aamupäivää ja tervetuloa Tampereen yliopistoon ja Kyberturvallisuusseminaariin!

Seminaarin järjestäjät ovat Tampereen yliopisto ja Pirkanmaan tietojenkäsittely-yhdistys PITKY ry sekä Tietotekniikan liitto.

Tampereella ja Pirkanmaalla on pitkä historia tietojenkäsittelyn eturintamassa olemisesta. Tampereen yliopistossa on ollut tietojenkäsittelyopin oppiaine jo vuodesta 1965 ja Pohjoismaiden ensimmäinen tietojenkäsittelyopin professuuri perustettiin silloiselle laitokselle vuonna 1967. Tässä välissä vuonna 1966 perustettiin puolestaan Pirkanmaan tietojenkäsittely-yhdistys PITKY ry.

Neljässä - viidessä vuosikymmenessä on otettu luonnollisesti suuria kehitysaskeleita alalla ja nykyään suuri osa kaikesta organisoidusta toiminnasta nojaa vahvasti tietojärjestelmiin ja tietoverkkoihin ja niiden jatkuvaan toimivuuteen.

Tietoturvasta on puhuttu jo pitkään, mutta viimeaikoina on havahduttu siihen että kyse ei ole ainoastaan huolehtimista tiedon ja järjestelmien turvallisuudesta vaan siitä että olemme nykyään niin riippuvaisia tietojärjestelmistä ja tietoverkoista että niiden tahallisella tai tahattomallakin sabotoinnilla on suoria vaikutuksia reaalielämään. Kyse on siis reaalimaailman kyberulottuvuudesta, eikä enää erillisistä ja irrallisista todellisuutta imitoivista sovelluksista tai virtuaalimaailmoista. Kyberturvallisuus on havaittu yhteiskunnan kannalta niin merkittäväksi tekijäksi, että sille ollaan luomassa nyt omaa strategiaa. Jotta olisimme vuonna 2016 kyberturvallisuudessa maailman huipulla, paljon asioita täytyy tehdä, myös käytännössä. Toivomme, että tämä seminaari toimii yhtenä edistäjänä kohti tätä tavoitetta.

Kun PITKY:n hallituksessa päätimme Kyberturvallisuus-seminaarin järjestämisestä katsoimme aiheen olevan meille uusi avaus, paitsi ajankohtainen niin myös kaipaavan lisää keskustelua ja yhteistyötä eri osapuolien välillä. Paitsi täällä Pirkanmaalla, niin myös koko Suomen mittakaavassa. Sen vuoksi lähestyimmekin Tietotekniikan liittoa ja alustavien keskustelujen perusteella myös TTL tukee seminaarin järjestämistä kattamalla osan kuluista.

Tilat ja järjestelyt eivät olisi kuitenkaan mitään ilman teitä, seminaarin puhujia ja osallistujia. Saimme varsin aikaisessa vaiheessa sovittua kaksi erittäin arvostettua keynote puhujaa, joiden ansiosta varmasti saimme ohjelman täyteen korkeatasoisia ja mielenkiintoisia esityksiä ja sitä kautta suuren joukon osallistujia, mikä ylitti odotuksemme. Tästä tuli suuri tapahtuma, käyttäkää se hyödyksenne, osallistukaa ja virittäkää keskustelua ja yhteistyötä.

Pidemmittä puheitta luovutan lavan seminaarin ensimmäiselle keynote puhujalle, Stonesoftin kyberturvallisuusjohtajalle, hyvät naiset ja herrat, Jarno Limnéll.

Mietteitä Tampereen kyberturvallisuusseminaarista , 10. Syyskuuta 2012

Juha-Matti Laurio, tietoturvakonsultti, Nixu Oy

Ajankohtaiseen kyberturvallisuuteen keskittyvä seminaari järjestettiin 6.9.2012 Tampereella. Seminaarin järjestäjätahoina olivat Pirkanmaan tietojenkäsittely-yhdistys Pitky ry, Tietotekniikan liitto ry ja Tampereen yliopiston informaatiotieteiden yksikkö. Aihe kokosi paikalle puhujat mukaan lukien yli 60 ammattilaista ympäri Suomea otsikolla Kyberturvallisuus, hyökkäys ja puolustus.

Kuluva syksy on omalla kyberturvallisuusrintamallamme sikäli mielenkiintoista aikaa, että Suomen virallisen kyberturvallisuusstrategian on tarkoitus valmistua vuoden loppuun mennessä.

Seminaarin keynote-puheenvuorot käsittelivät kyberturvallisuutta strategisesta näkökulmasta sekä kyberturvallisuuden koulutuksen linkittymistä informaatioturvallisuuden koulutukseen.

Kyberturvallisuusjohtaja, puolustusvoimista teollisuudenalalle siirtynyt Jarmo Limnell aloitti puheenvuoronsa nimeämällä kyberturvallisuuden malliesimerkiksi kokonaisturvallisuudesta, joka koskettaa niin julkista sektoria, yksityistä sektoria kuin jokaista suomalaistakin.

Limnell arvioi Suomenkin joutuvan merkittävän kyberhyökkäyksen kohteeksi parin vuoden sisällä. Kuten seminaarissa mukana ollut kollega Olli Haukkovaara Nixusta kommentoikin: Suomen tunnettavuus tietoturvallisena maana voi tehdä meistä jollekin valtiolle tai rikollisorganisaatiolle houkuttelevan testipenkin – jos Suomen infrastruktuuriin on hyökättävissä on helppo saada polvilleen mikä tahansa maa.

Kybermaailmasta pelisäännöt puuttuvat vielä pitkälti, vaikka esimerkiksi hyökkäykselliseen tarkoitukseen tehtyjä haittaohjelmia on olemassa jo useilla valtioilla. Keynoten yksi kysymyksistä olikin voisiko Suomi toimia eräänlaisena kyberrauhanvälittäjänä mm. rakentamalla digitaalisen maailman normistoja.

Luennossa käsitellyn tilannetietoisuuden ylläpitämisen ja siihen liittyvän konkreettisen tilannekuvan tärkeyttä ei voi koskaan korostaa liikaa. Mm. eilen näimme käytännössä että suomalaisiin verkkolehtiin kohdistuneen verkkohyökkäyksen lähteistä oli liikkeellä ristiriitaista ja nopeasti vaihtuvaa tietoa.

Koulutusasioihin keskittynyt Jyväskylän yliopiston tutkija Martti Lehto, eläkkeellä oleva ilmavoimien eversti, kävi läpi alan evoluutiota nimeten Blaster-verkkomadon yhdeksän vuoden takaa aikansa kyberaseeksi. Toinen esimerkeistä oli Yhdysvaltain DHS:n kokeilu vuodelta 2007. Tuolloin Aurora-projektissa demonstroitiin voimalaitoksen generaattorin tuhoamista verkon yli.

Jyväskylän yliopistossa käytetty kybermaailman jaottelu noudattelee keväisen, blogissammekin mainitun Viiden minuutin sota -keskustelun terminologiaa.

> *Hyvä kysymys onkin kuinka keskivertokansalainen, muualla kuin it-alalla toimivana määrittelisi kybervandalismin?*

Tietoverkkorikoksista puhutaan iltauutisissa useinkin, mutta pitäisikö puhua kyberrikoksista?

Onko identiteettivarkaus rivikansalaiseen kohdistuva kyberhyökkäys

Tutkija Anna Leppänen Poliisiammattikorkeakoulusta Tampereelta taustoitti tietoverkkorikollisuuden tutkimusta käsittelevää luentoaan luvuilla poliisin tilastoimista tietotekniikkarikoksista. Vaikka tilastoinnissa on haasteita ja tietotekniikkaa välineenä käytettävän rikoksen määritteleminen on vaikeaa, oli luvuissa

selvä nousu. Seminaariin mennessä paikallispoliisin tilastoihin tänä vuonna keräämä luku oli reilusti yli 800. Koko viime vuonna määrä oli selkeästi pienempi, 332 kappaletta. Mitä tämä kertoo osaltaan kyberrikollisuuden kasvusta?

Laajalti ympäri kenttää esitetty toive on keskitetyn tilannekuvaratkaisun saaminen maahamme. Tilannekuvaan liittyy olellisesti SIEM (Security Information and Event Management) – tietoturvaan liittyvän tiedon ja tapahtumien hallinta, jota käsitteli Insta DefSecin esitys.

Riippumatta siitä osallistuistko seminaariin vai et olisi mukava kuulla ajatuksiasi aiheesta. Keskustelua voi jatkaa kommentoimalla, LinkedInin suomenkielisessä Kyberturvallisuus-ryhmässä tai Twitterissä hashtagilla #kyberturvallisuus.

Verhojen raottamista verkkosodan harjoitteluun

Ehdottomasti teknisintä antia seminaarissa oli Baltic Cyber Shield 2010 -harjoitukseen osallistuneen Jussin esitys. Voiton vieneeseen Blue 5 -tiimiin kuulunut penetraatiotestaaja oli valittu tiimiin vapaaehtoisena eräältä pieneltä postituslistalta. Harjoitus sijoittui mm. simuloituun ydinvoimalaympäristöön. Kuulimme mm. ilmaisia vinkkejä Windowsin tiettyjen rekisterihaarojen seuraamisen tärkeydestä ja penetraatiotiimin keskinäisestä kommunikoinnista. Kun tekijät tunsivat toisensa pitkältä ajalta oli kommunikointikin melkeinpä tiimikollegan kasvonpiirteistä päättelyä – saattoi siis luottaa että toinen tekee oman osuutensa perään katsomatta.

Seminaarin päättäneen paneelikeskustelun johdantona oli ”Millaista tutkimusta, koulutusta ja projekteja aiheen ympärille pitäisi rakentaa”?

Paneelikeskustelun johtopäätöksenä todettiin, että vakavasti otettavan kyberturvallisuusosaajien joukon saamiseksi Suomeen mm. yliopistotasoisen koulutuksen määrää tulisi kovastikin lisätä.

Usealla maalla on kasassa vapaaehtoisista koottuja, usein nuorista alan osaajista koostuvia “kybervalmiusryhmiä”. Tällaisen ryhmän tärkeyttä meilläkin korostettiin, onhan ikävää jos todellisia osaajia siirtyy pahalle puolelle mielekkäiden tehtävien puuttuessa. Myös mahdolliset synergiaedut maanpuolustusjärjestöjen kanssa tehtävän yhteistyön myötä nousivat kommenteissa esiin.

Seminaarissa esitettiin myös monia muita kyberturvallisuuden aihetta eri näkökulmista käsitteleviä esityksiä, joiden esityskalvot on koottu tässä seminaarijulkaisussa yhteen. Juha-Matti Laurio on käsitellyt kyberturvallisuusseminaaria ja muita mielenkiintoisia aiheita Nixu Oy:n tietoturvablogissa http://www.nixu.fi/blogi/2012/syyskuu/mietteita-tampereen-kyberturvallisuusseminaarista-osa-i/

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Strateginen näkökulma kyberturvallisuuteen – kehityssuunta on huolestuttava

Jarno Limnéll, ST, Director of Cyber Security, Stonesoft

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

Strateginen näkökulma kyberturvallisuuteen – kehityssuunta on huolestuttava

Jarno Limnéll, director of cyber security, sotatieteiden tohtori, Stonesoft Oyj

Esityksessään Jarno esittää, että kyberturvallisuus on digitaalisen maailman turvallisuutta. Se tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tuotettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoituvasti hallita, ja tarvittaessa sietää, kyberuhkia ja niiden vaikutuksia. Kyberturvallisuuden käsitettä tulisi myös popularisoida ja saattaa se osaksi ihmisten jokapäiväistä arkea.

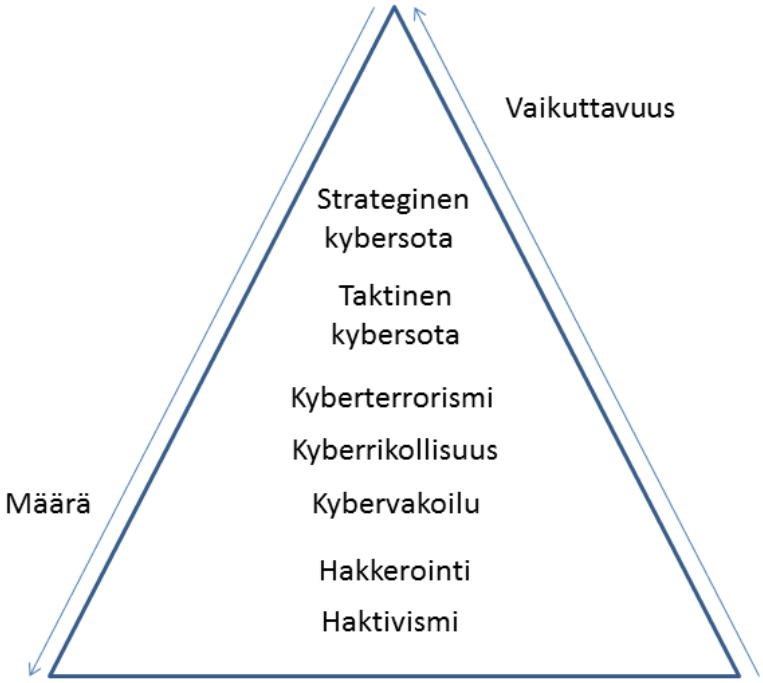
Kyberturvallisuus ja valtioiden kyvykkyys sen hallinnassa riippuu valtion omien toimijoiden lisäksi kansalaisista jotka kykenevät innovatiivisesti kehittämään omia kykyjään. Eräässä black hat seminaarissa Yhdysvaltolainen korkea upseeri oli todennut osallistujille että seminaarissa istuu Yhdysvaltojen tulevaisuuden turvallisuuden tekijät.

Turvallisuus on ensisijaisesti tunne.

Jarno esittää esityksessään viisi huolestuttavaa kehityssuuntaa.

1. Kybersota ja kilpavarustelu (Esimerkkejä lehtileikkeistä: 1. Israel prepared for 30 day war with Iran, 2. US general: we hacked the enemy in Afghanistan, 3. UK spy agencies urged to wage war on cyber enemies). Esim Israel valmistautuisi sotaan digitaalisella tykistöllä ensi iskuna. (Esimerkki lehtileikkeistä: DARPA looks to make cyberwar routine with secret “plan X”).
    a. Hyökkäyksellisten aseiden kehitykseen kohdennetaan yhä enemmän ja enemmän varoja.
    b. Koska kybervarustelu ei ole näkyvää, arvailu vastustajan kyvyistä kiihdyttää (peliteorian mukaan) omaa varustautumista.
2. Uhkan kaava, kyber
   aikomus x kyky x riippuvuus = uhka
   Aikomus lisää uhkaa, kyvyt lisäävät uhkaa (niin valtiolliset kuin ei valtiolliset toimijat), riippuvuus lisää uhkaa (riippuvuudella tarkoitetaan haavoittuvuutta, eli sitä miten riippuvainen yhteiskunta on digitaalisen maailman turvallisuudesta). Suomea voidaan pitää yhtenä ehkä riippuvaisimpana valtiona maailmassa.

3. Dynaaminen uhkakenttä



4. Pelotevaikutusten vaikeus ja sivuvaikutukset
   Valtiolla on vaikeutta luoda uskottavaa pelotetta jos kyvykkyys pidetään piilossa. On oletettavaa että kykyä on jatkossa pakko osoittaa avoimemmin. Kyvykkyyksiin liittyy lisäksi ennalta arvaamattomia sivuvaikutuksia.
5. Välinpitämättömyys kyberturvallisuutta kohtaan ja uhkien vähättely (jopa kieltäminen) on hyvin huolestuttavaa

Jarno esittää myös 10 strategisen tason vaatimusta, mitä Suomen pitäisi ottaa huomioon varmistaakseen kyvykkyytensä kyberturvallisuuden alalla:

1. kyberturvallisuus on malliesimerkki kokonaisturvallisuudesta
   a. julkinen sektori – yksityinen sektori – jokainen suomalainen (yhteiskunnassa).
2. Paradigman muutos
   a. strategisen turvallisuusymmärryksen ja ohjaavuuden välttämättömyys (valtio, yritys)
3. Paradigman muutos
   a. turvallisuuden illuusion rikkominen
   b. turvallisuus ei voi olla enää jälkiajatus digitaalisessa maailmassa. Turvallisuuden pitää olla mukana alusta lähtien.
4. Teknologisen osaamisen lisääminen ja innovatiivisuuden hyödyntäminen
   a. vahva teknologia ja soveltamisosaaminen
   b. suomalaisiin luotetaan ja kyberturvallisuus perustuu nimenomaan luottamukseen.
   c. käsite ”viiden sekunnin sota”
5. Haavoittuvuuksien mininmointi ja ymmärtäminen. Haavoittuvuuden vähentäminen edes minimitasolle. On kiinnitettävä huomiota haavoittuvuuksien perussyihin eli pitää ymmärtää mistä haavoittuvuudet johtuu.

6. Dynaaminen uhkaympäristö edellyttää dynaamisia ratkaisuja
    a. staattinen ja jäykkä puolustusratkaisu ei toimi
7. Tilannetietoisuus ja ymmärrys
    a. NATOn Smart Defence konsepti
    b. puolustusvoimauudistus
    c. kyberturvallisuus
    d. keskitetty hallinta, johtaminen ja ennakoittavuus
8. Resielienssi, sietokyky, kestokyky, kyky sietää erilaisia häiriötilanteita ja toipua niistaä mahdollisimman nopeasti, toimenpiteiden ennakointi
9. Offensiivisen ajattelun ja kyvykkyyden tärkeys
    a. puolustuksellinen kyky, sietokyky, hyökkäyksellinen kyky. Kyse ei ole siitä tarvitsemmeko hyökkäyksellistä kyberkykyä vai emme, vaan miten hankimme sen
10. Suomi kyberrauhanvälittäjäksi
    a. kansaivälisisesti varsin neutraalina pidetyllä Suomella olisi nyt mahdollisuus aloitteellisesti ajaa digitaalisen maailman normiston rakentamista, siis toimia kyberrauhanvälityksen edistämisen suurvaltana. Tällainen rooli sopisi meille.

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

iKyber: Kyberturvallisuuden johtamisjärjestelmä

Juha Högmander, Project Manager, GSEC, Insta DefSec Oy

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

iKyber: Kyberturvallisuuden johtamisjärjestelmä

Juha Högmander

Project Manager, GSEC

Insta DefSec Oy

Aiheet

- Yritysesittely
- Insta kyberkumppanina
- Kyberturvallisuus
- Kybertoimintaympäristö
- Tarve iKyber-järjestelmälle
- iKyber-järjestelmän toiminnallinen perusajatus
- iKyber-järjestelmän toiminnalliset komponentit
  - Kyberturvallisuuden ylläpito
  - Kybertilannekuva ja analysointi
  - Kybersuojausmenetelmät
- Yhteenveto

Insta Group ja Insta DefSec Oy

Insta Group

- Insta Group Oy on perheyritys, jonka juuret ulottuvat vuoteen 1960. Nykyään meillä työskentelee jo noin 700 osaajaa innovatiivisten tuotteiden, ratkaisujen ja palvelujen parissa
- Vahvan kasvun ja kansainvälistymisen aikaa elävä yritys on erikoistunut kahteen toimialaan, jotka ovat:
  - puolustus- ja turvallisuusteknologia (Insta DefSec Oy)
  - teollisuusautomaatioteknologia (Insta Automation Oy).

Insta DefSec Oy

- Insta DefSecin yli 300 henkilöstä noin 250 työskentelee tehtävissä, jotka liittyvät turvallisuusviranomaisten järjestelmien, vahvan tietoturvan sekä palvelutuotannon tarjoamiseen.

INSTA DefSec

Insta kyberkumppanina

INSTA DefSec

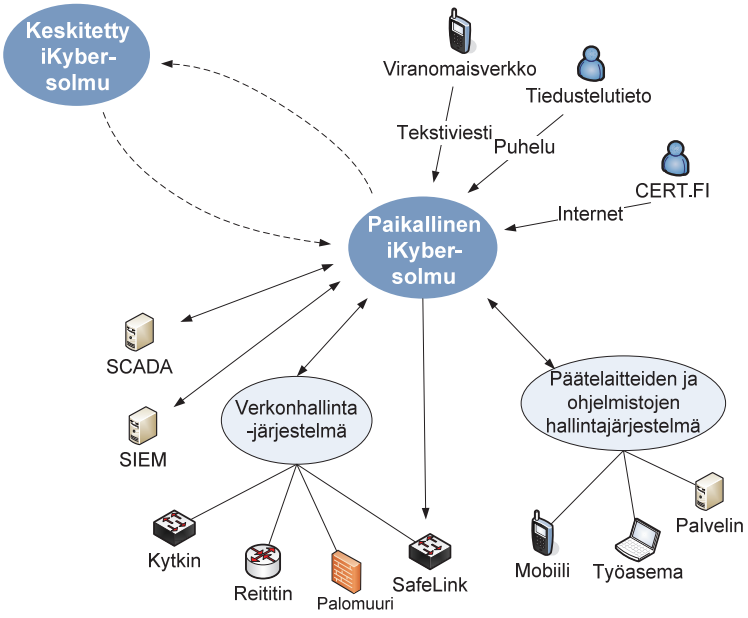
Kyberturvallisuus

Määritelmiä:

- ”Kyberturvallisuudella tarkoitetaan pääsääntöisesti yhteiskunnan (elintärkeiden) toimintojen ja väestön hyvinvoinnin suojaamista kyberavaruuden kautta tulevia hyökkäyksiä vastaan.”
  - ”Kyberturvallisuus ei ole synonyymi tietoturvallisuudelle, verkkoturvallisuudelle, atk-turvallisuudelle, tai millekään muulle turvallisuustermille”
  - ”Yksi – mutta ei ainoa – suojattava kohde on tieto. Tässä on siis rajapinta tietoturvallisuuteen.”
- ”Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen ulottuvuus.”
  - Kyberpuolustus termin määritelmä poikkeaa kyberturvallisuudesta näkökulmansa osalta.

Kybertoimintaympäristö

Kybertoimintaympäristö

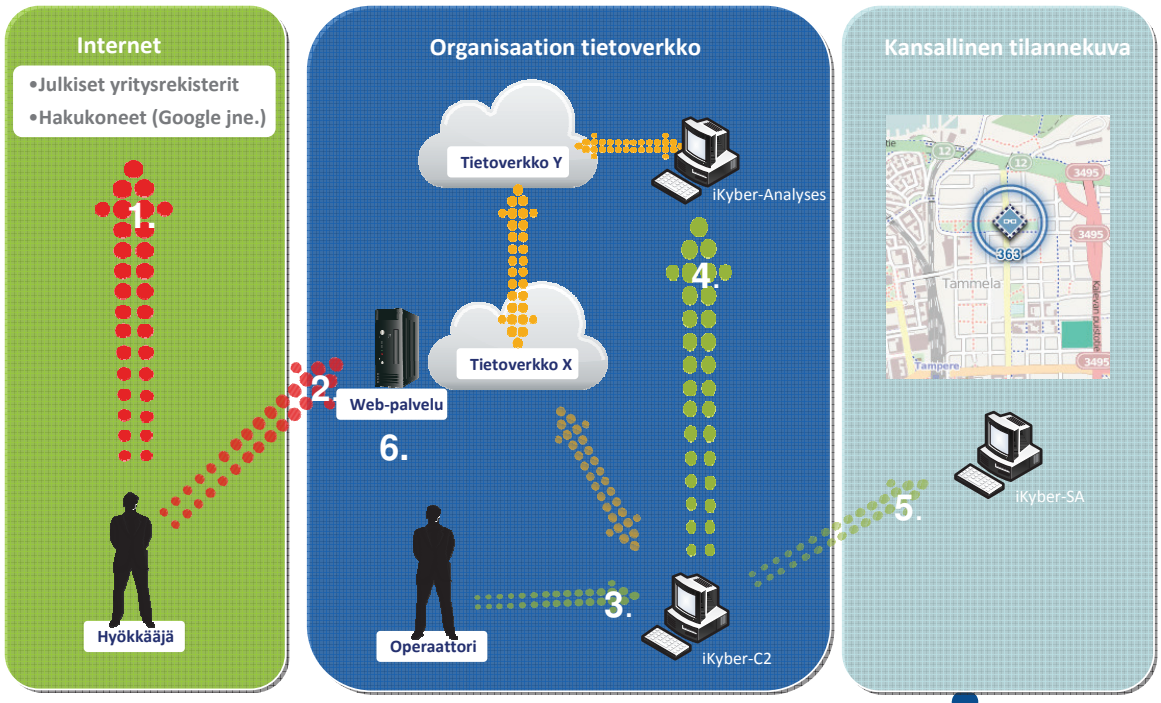


- Johtaminen
- Toimintakyky
- Sensorit
- Ulkopuolinen informaatio
- Hallinta
- Suojausmekanismit
- Korjausmekanismit

Tarve iKyber-järjestelmälle

- ”On olemassa tarve operatiivisen tason kyberturvallisuuskeskukselle”, Catharina Candolin, Pääesikunta, tietoverkkopuolustussektorin johtaja
- ”Valtakunnallisesti haasteena on keskitetysti johdettu kyberpuolustus, jolla olisi valvontakyky riittävällä laajuudella ja mahdollisuus vastatoimiin.”
- ”Tarvitaan keskitetty johtamiskyky ja hajautettu vaikuttamiskyky”
- ”Tarve kyberjärjestelmälle yksittäisen toimijan näkökulmasta on pystyä suojautumaan samoja merkittäviä kyberuhkia vastaan kuin valtakunnallisesti”

Tarve iKyber-järjestelmälle: Case - Kriittisen toimintakyvyn ylläpito



Yhteenveto

- Kysymyksiä tai ajatuksia

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Miten Suomeen saatiin maailman puhtaimmat verkot

Jani Kenttälä, Clarified Networks Oy, part of Codenomicon Group

CIRCMI

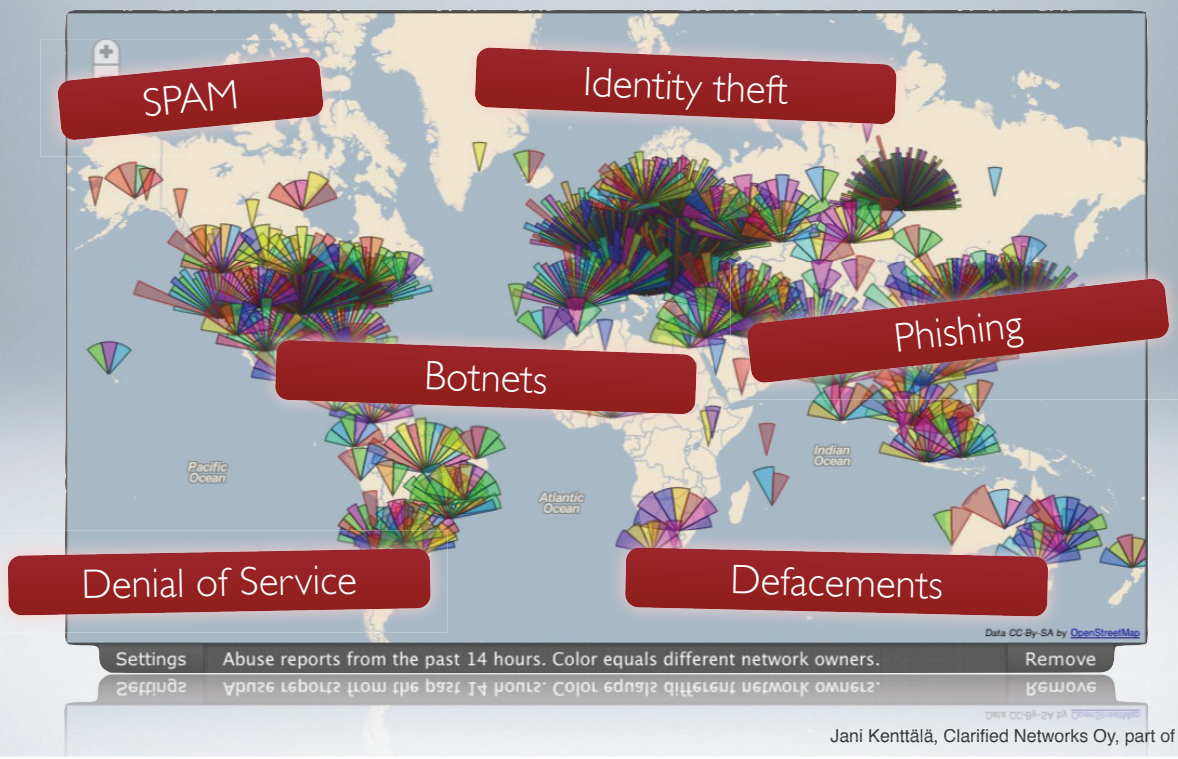
6. syyskuuta 2012

Tampereen yliopisto

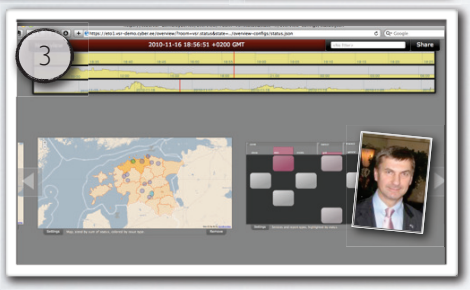
P/I/T/K/Y

ABUSE TILANNEKUVAT

KUINKA SUOMEEN SAATIIN MAAILMAN PUHTAIMMAT VERKOT



Jani Kenttälä, Clarified Networks Oy, part of Codenomicon Group

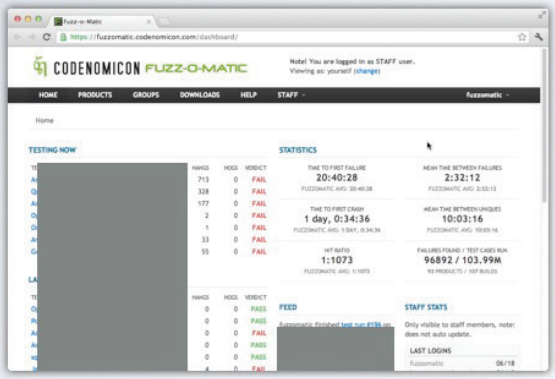


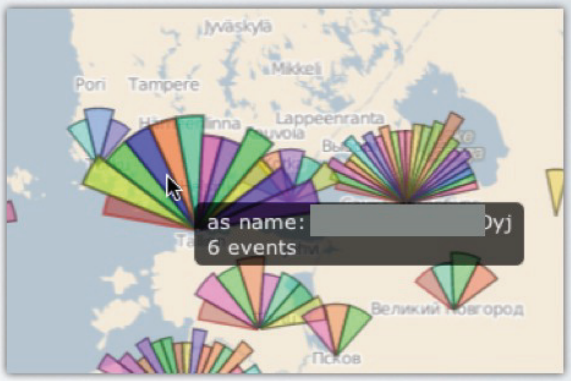
1. White House still remembers our research results from 2002, Chief of Defense Command Finland tweets about it after his visit. (Clarified Networks and Codenomicon are spin-offs from Oulu University Secure Programming Group).
2. Analyzer used in Bredolab botnet takedown, Dutch TV-channel covers

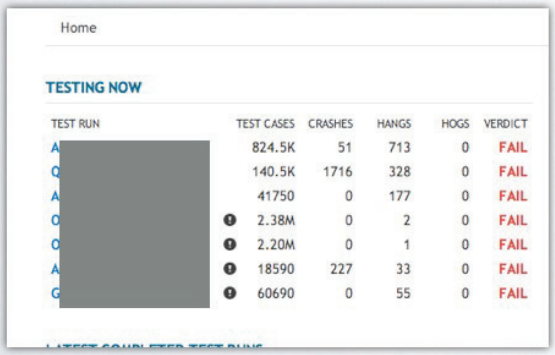
   Mikko Hyppönen (F-Secure) and Bob Burls (eCrime-unit in UK) keynote, Analyzer used to visualize evidence against m00p gang.
3. Critical Infra SA deployment for the Estonian Government
4. Situation rooms for NATO CCDCOE cyber exercises.
5. Clarified Visualization in Mikko Hyppönen's TED talk, 500 000 views as of 2011-09
6. News coverage of CERT.be fighting against website hacks, TV-premiere for our abuse handling tools.

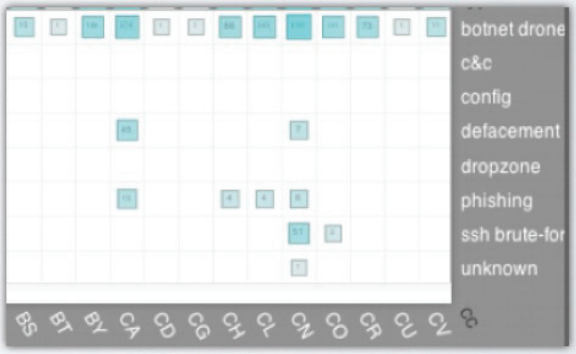
SOME PUBLIC EVENTS

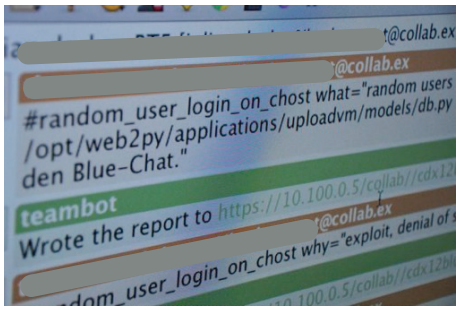
OUR TOOLS FIND SOFTWARE DEFECTS/VULNERABILITIES AND **REAL** SECURITY INCIDENTS





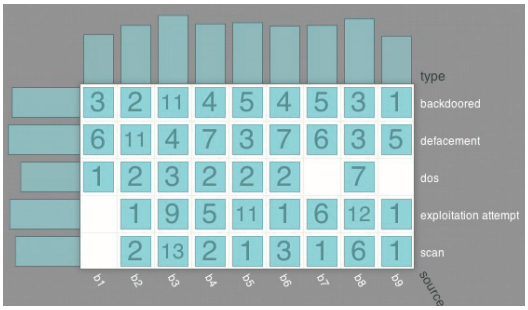






Blue team microblog-style real-time reports

Red team campaign reports



Report visualizations

IDS alert visualizations

Network traffic analysis & visualization tools

Visual situation briefings up to the PM level.

LOCKED SHIELDS

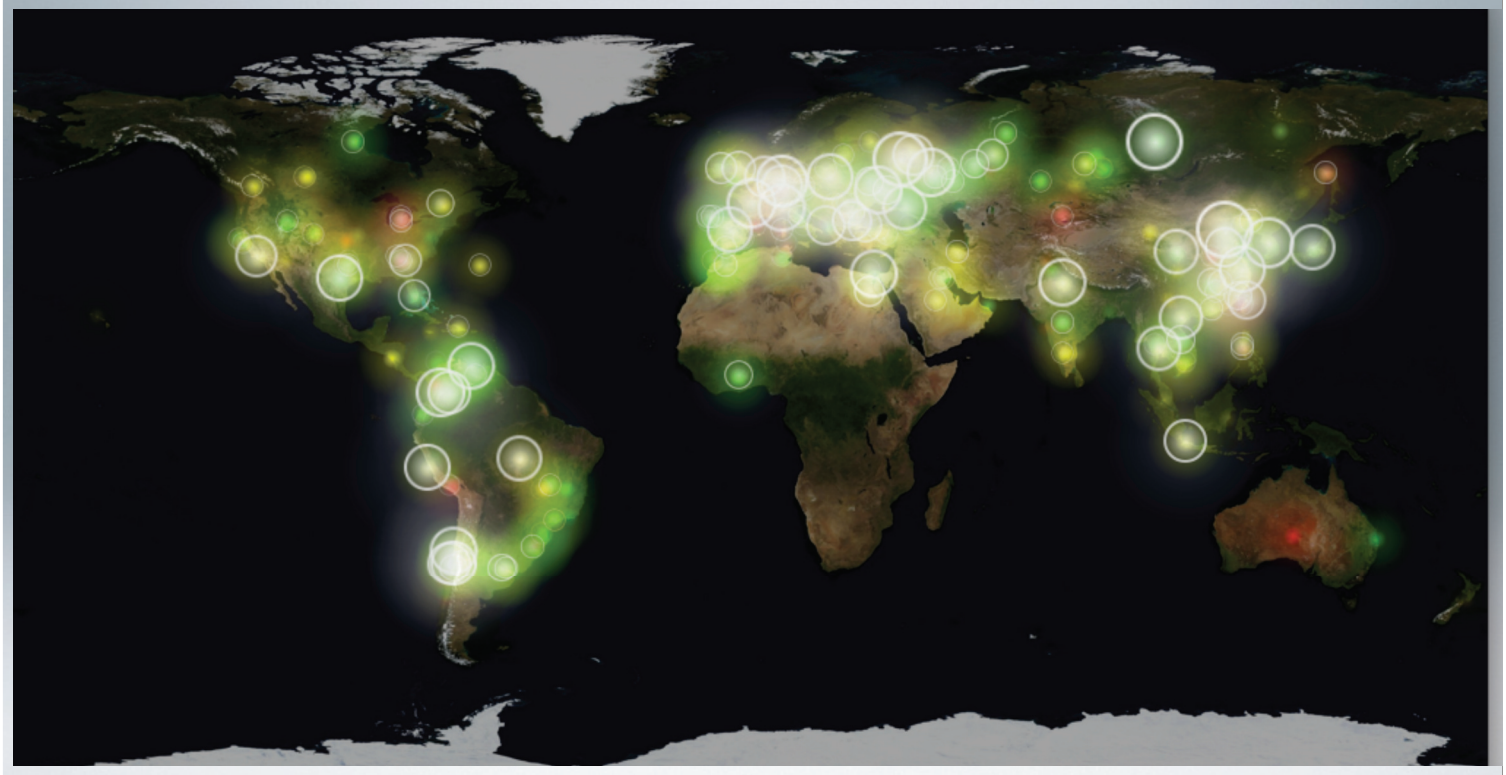
We implemented the situation rooms for NATO's *Locked Shields* cyber defence exercise. Our tools visualized network traffic, security alerts and microblog-style reports from security teams.

CHALLENGE AS PRESENTED BY MIKKO HYPPÖNEN IN TED

http://www.youtube.com/watch?v=cf3zxHuSM2Y

5m 25s - breeding of malware (F-secure finds tens of thousands of malware variants each day)
9m 06s - criminal infra constantly being evacuated to new locations (Mikko uses our visualization to demonstrate)

TRADITIONAL METHODS ARE NOT SOLVING THE PROBLEM



A real-time visualization showing current abuse situation.

CERT FINLAND 2005:

HOW TO GAIN SITUATION AWERENESS ABOUT INCIDENTS OCCURING IN FINNISH NETWORKS?

ABUSE FEEDERS ALREADY KNOW

Feeders produce data, which

Abuse Feeds / Intelligence

- Non-profit and commercial organizations
- Shadowserver, Zone-H, DShield, Abuse.ch, Malwaredomainlist and tens of more.

AbuseSA users collect, process and report systematically

Proxies

- National and Governmantal CERTS
- Cyber Defence Organizations
- ISP Abuse Teams

Cleaners

- ISPs
- Critical Infrastructure Providers
- Large Enterprises

to protect

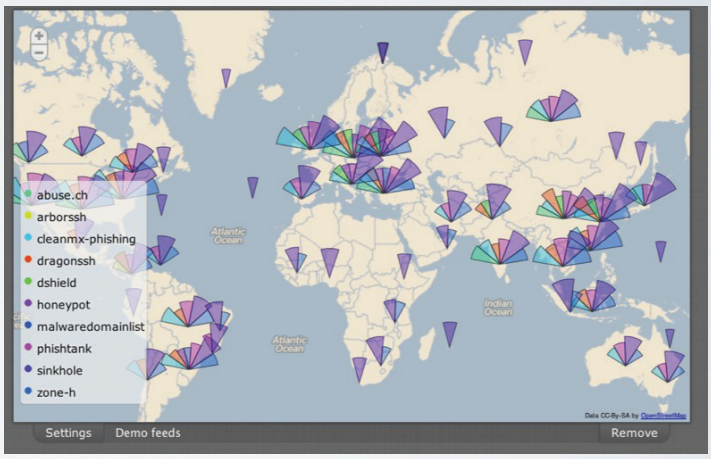
Citizens

Critical Infra

A DAY WORTH OF DATA

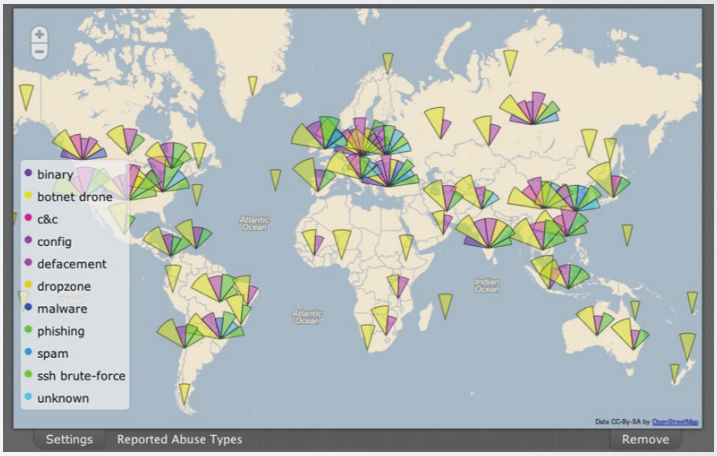
71000 abuse reports, 2600 network owners, by using a limited set of demo feeds

- *abuse.ch* = crimeware tracking (zeus, spyeye, palevo)
- *arborssh, dragonssh* = monitoring ssh brute force attack sources
- *(project) honeypot* = content spammers
- *phishtank* = sites used for identity theft
- *zone-h* = defaced sites
- *sinkhole* = botnet drones trying to connect to the c&c, now in posession of the security community



DIFFERENT ABUSE TYPES

- *c&c* = botnet command and control
- *phishing* = websites used for identity theft
- *defacement* = websites compromised for embarrasment and propaganda
- *ssh brute-force* = operating system compromised and used as jumping point for further criminal activity
- *malware, binary, config, dropzone* = compromised sites used for further compromises



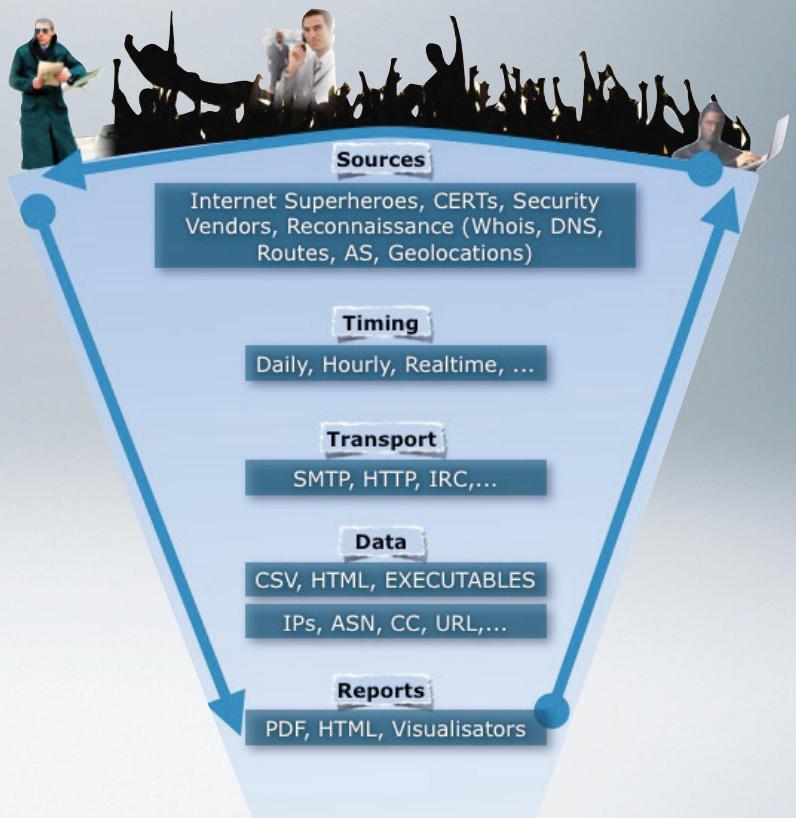
RAISING THE MATURITY OF ABUSE HANDLING

UP TO THE FULL AUTOMATION

- Manual
- Ad hoc (in-house) scripts
- Hands on automata (abuse specific ticketing systems)
- **Hands off automata**
- Investigative capability

WHY THIS HASN'T BEEN DONE EARLIER?

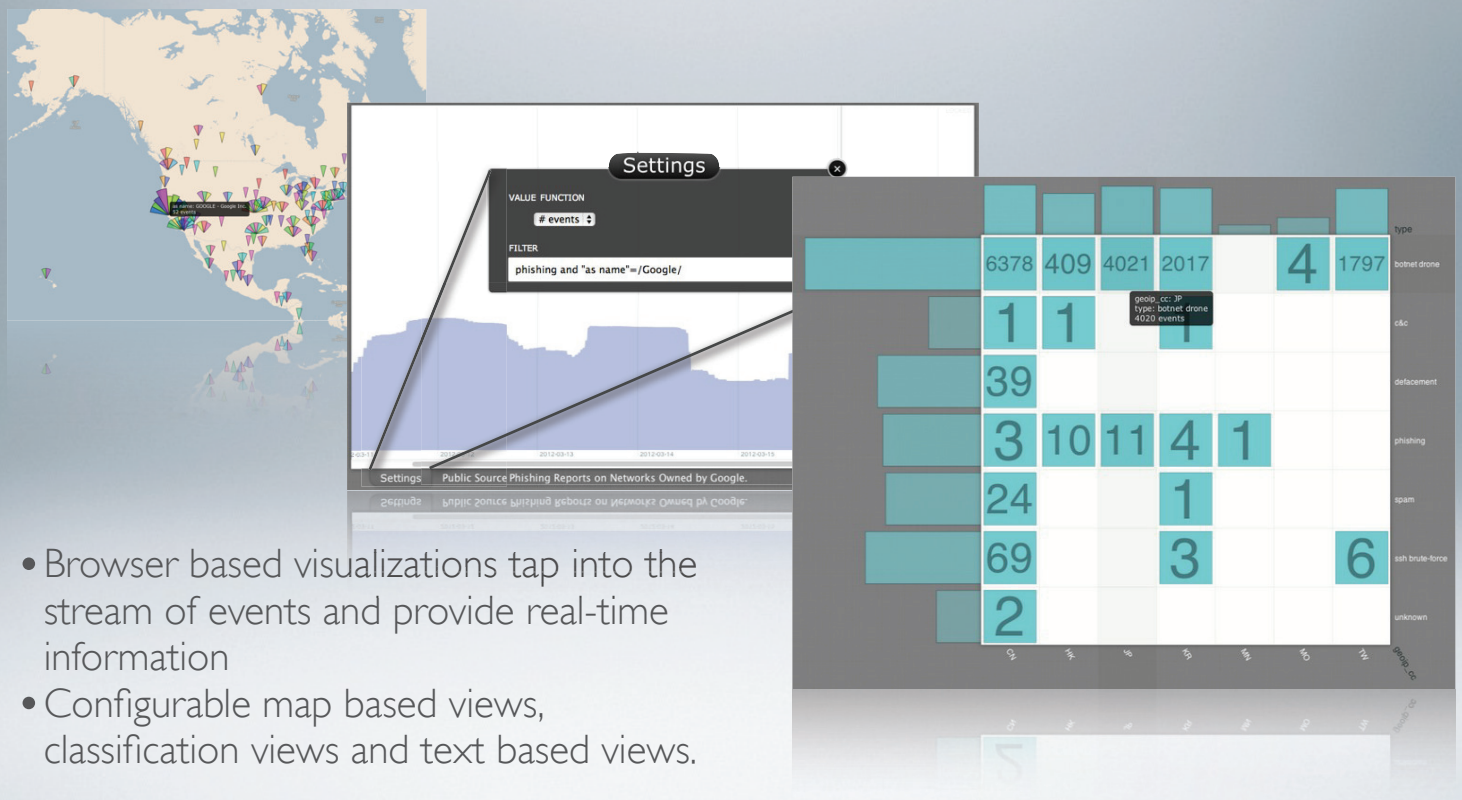
- Each feed is different in terms of timing, transport, data format, data content, reliability etc.
- On the other hand, reporting requirements may be very specific.
- -> Innovation required



INNOVATION TURNED INTO A SOFTWARE

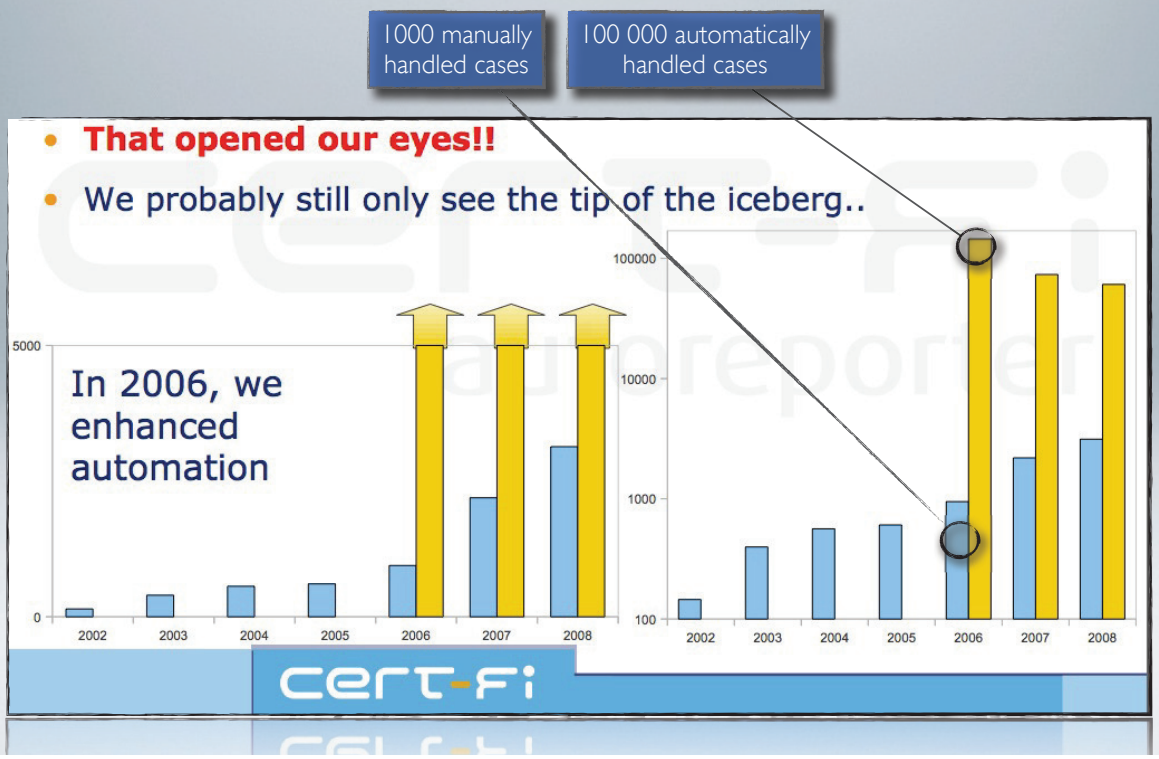
- Botnet inspired architecture
  - Distributed
  - Modular
  - Bot for each specific task
    - Build for various feed formats, download mechanisms, augmenting, sanitizing, normalizing, reporting.
- Inspired by **6** CERT-FI and **2** CERT-EE generations of abuse handling automata
- **Fully automatic**

VISUALIZATIONS



- Browser based visualizations tap into the stream of events and provide real-time information
- Configurable map based views, classification views and text based views.

EFFICIENCY TROUGH AUTOMATION



OTHERS SAW IT TOO

Microsoft | Security

TechNet Blogs > Microsoft Security Blog > Finale – Lessons from Some of the Least Infected Countries in the World – Part 6

Finale – Lessons from Some of the Lea
Malware Infected Countries in the Wor
Part 6

Tim Rains – Mic

In this final post in th
I share some key findings

My previous five blog posts in this series focused on the threat landscape and insig
security professionals in Austria, Finland, Germany, and Japan. All three

CSO SECURITY
Data Pr
News Blogs Tools

Home » Data Prot

NEWS

Nations
ISPs

Austria, Finland, Germany and Japan top for security

Security on msnbc.com
Solution Centers White Papers Webcasts Podc

Who's got the world's 'cleanest' computers?

Finland leads as country with lowest rate of malware

"The infection rates and other metrics for Finland have consistently been below the world-wide averages, and we have often wondered ourselves what the reason is for this"

– Kimmo Bergius, Microsoft's Chief Security Advisor

Using the yardstick of computers cleaned per mile (CCM)*, Austria

Network security bas
Computer incident de
A few good IT securit
Map of data breach d
IT risk assessment fr
How to do end-to-en
How to compare and

contacting users they believe to be infected as soon as they notice problem traffic and if necessary disconnecting them until the issue has been addressed. National CERT bodies, meanwhile, go out of their way to support ISPs with up-to-date threat lists drawn from honeynets, darknets and automated malware analysis tools, distributing this data as a matter of course.

Finland is known as having networks with the fewest malicious software (malware) infections, and within Finland, the telecommunications company TeliaSonera prides itself in being the "**cleanest of the clean**."
--Microsoft Case Study

ABUSE SA REPORT

Statistics (can be tailored, example provides AS + Type statistics for North America)

15153	STARWIRELESS-15153 - Star Wireless, Inc.	botnet drone	2
15162	CRICKETCOMM - Cricket Communications Inc	botnet drone	7
15169	GOOGLE - Google Inc.	phishing	57
15198	CCPI---SITE-1 - Convention Communications Provisioners, Inc.	botnet drone	8
15206	MDSG-PACWEST - Pac-West Telecomm, INC.	botnet drone	15
15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	phishing	3
15247	RADIANT-VANCOUVER - Radiant Communications Ltd.	botnet drone	9
15250	USFAMILY-ASN - USFamily.net	botnet drone	2
15267	702COM - 702 Communications	botnet drone	3

ABUSE SA REPORT

Details

7184	2012-06-11 03:40:39 UTC	phishtank	phishing	67.212.175.138	32475	SINGLEHOP-INC - SingleHop	US	Phishing at http://www.paypal.com.cgi-bin-webscr-cmd-login-submit-dispatch-5885d2636.903
7185	2012-06-11 03:25:03 UTC	phishtank	phishing	67.212.175.138	32475	SINGLEHOP-INC - SingleHop	US	Phishing at http://www.paypal.com.cgi-bin-webscr-cmd-login-submit-dispatch-5885d2636.903
7186	2012-06-11 03:05:46 UTC	phishtank	phishing	67.212.175.138	32475	SINGLEHOP-INC - SingleHop	US	Phishing at http://www.paypal.com.cgi-bin-webscr-cmd-login-submit-dispatch-5885d2636.903
7187	2012-06-11 03:05:46 UTC	phishtank	phishing	148.235.138.83	8151	Uninet S.A. de C.V.	MX	Phishing at http://www.arpapel.com.mx/images/.../ppl_dk/webscr.htm, IP: 148.235.138.83
7188	2012-06-11 03:06:17 UTC	phishtank	phishing	69.73.145.12	11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc	US	Phishing at http://paypal.com.us.cgi-bin.webscr.cmd.login-run.5885d80a13c0db1f8e263663d3
7189	2012-06-11 03:06:17 UTC	phishtank	phishing	67.212.175.138	32475	SINGLEHOP-INC - SingleHop	US	Phishing at http://www.paypal.com.cgi-bin-webscr-cmd-login-submit-dispatch-5885d2636.903

kyberturvallisuus
hyökkäys ja
puolustus

seminaari 6.9.2012

Baltic Cyber Shield 2010

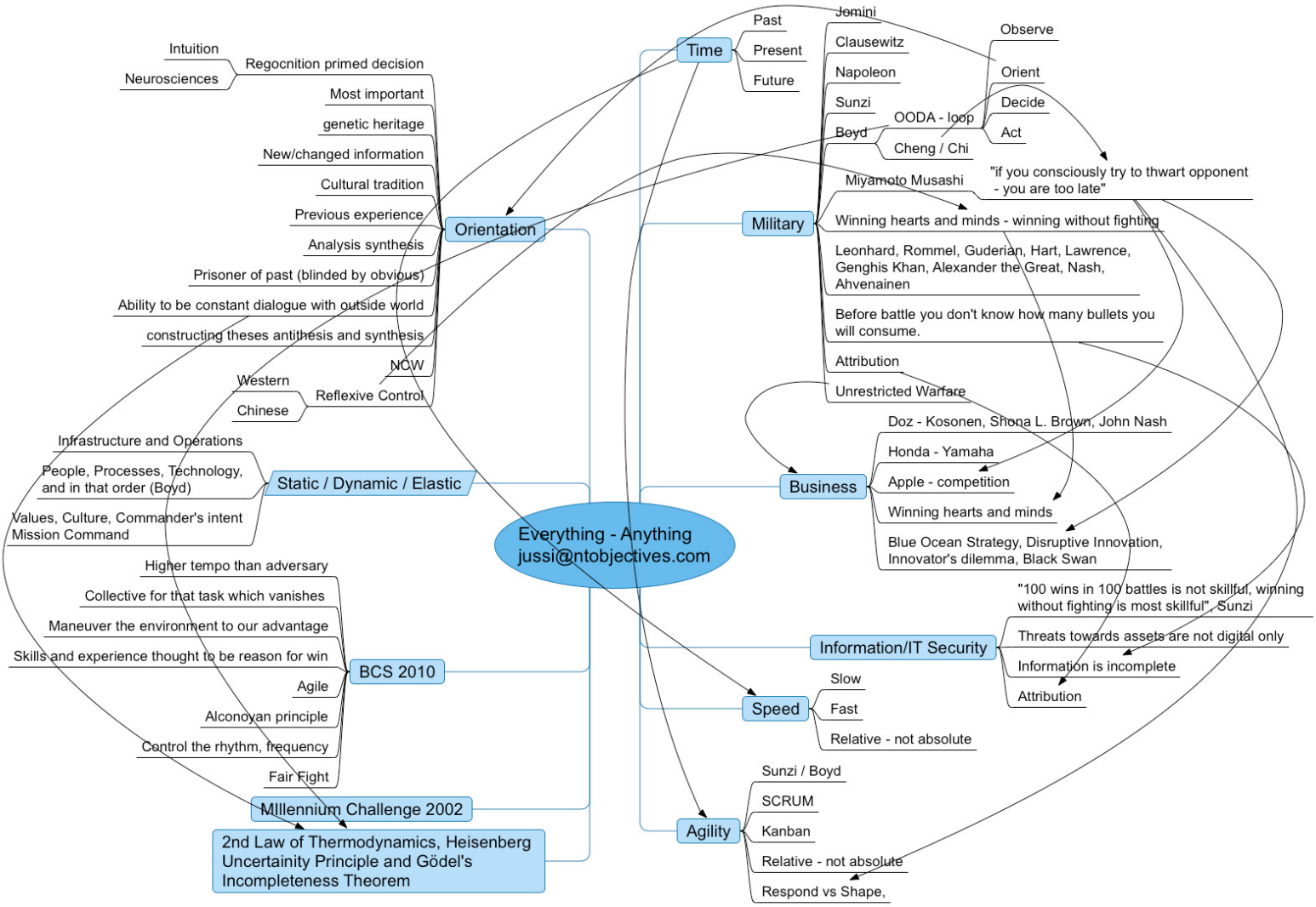
Jussi, Blue team 5

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y


Everything - Anything
jussi@ntobjectives.com
Time
Past
Present
Future
Orientation
Intuition
Neurosciences
Regocnition primed decision
Most important
genetic heritage
New/changed information
Cultural tradition
Previous experience
Analysis synthesis
Prisoner of past (blinded by obvious)
Ability to be constant dialogue with outside world
constructing theses antithesis and synthesis
NOW
Western
Chinese
Reflexive Control
Military
Jomini
Clausewitz
Napoleon
Sunzi
Boyd
OODA - loop
Cheng / Chi
Observe
Orient
Decide
Act
"if you consciously try to thwart opponent - you are too late"
Miyamoto Musashi
Winning hearts and minds - winning without fighting
Leonhard, Rommel, Guderian, Hart, Lawrence, Genghis Khan, Alexander the Great, Nash, Ahvenainen
Before battle you don't know how many bullets you will consume.
Attribution
Unrestricted Warfare
Business
Doz - Kosonen, Shona L. Brown, John Nash
Honda - Yamaha
Apple - competition
Winning hearts and minds
Blue Ocean Strategy, Disruptive Innovation, Innovator's dilemma, Black Swan
Static / Dynamic / Elastic
Infrastructure and Operations
People, Processes, Technology, and in that order (Boyd)
Values, Culture, Commander's intent Mission Command
BCS 2010
Higher tempo than adversary
Collective for that task which vanishes
Maneuver the environment to our advantage
Skills and experience thought to be reason for win
Agile
Alconoyan principle
Control the rhythm, frequency
Fair Fight
Information/IT Security
"100 wins in 100 battles is not skillful, winning without fighting is most skillful", Sunzi
Threats towards assets are not digital only
Information is incomplete
Attribution
Speed
Slow
Fast
Relative - not absolute
Agility
Sunzi / Boyd
SCRUM
Kanban
Relative - not absolute
Respond vs Shape,
MIllennium Challenge 2002
2nd Law of Thermodynamics, Heisenberg Uncertainity Principle and Gödel's Incompleteness Theorem

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Kyberturvallisuus ja informaatioturvallisuuden koulutus

Martti Lehto, ST, ev evp., Jyväskylän yliopisto

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

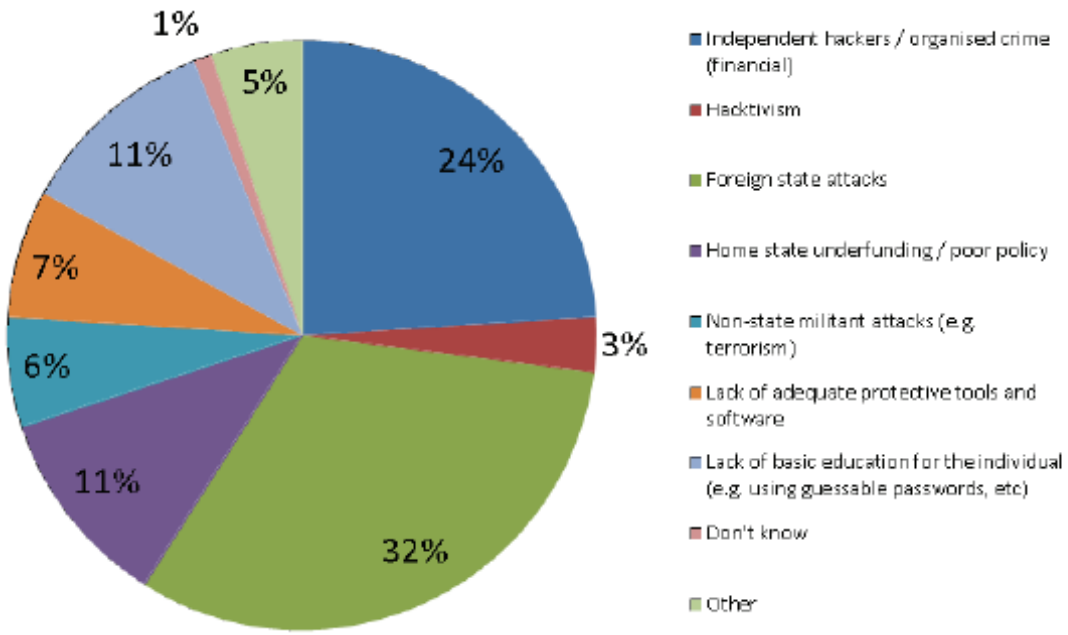
JYVÄSKYLÄN YLIOPISTO

Kyberturvallisuus ja informaatioturvallisuuden koulutus

Kyberturvallisuus, hyökkäys ja puolustus, PITKY ry:n seminaari, Tampere

JYVÄSKYLÄN YLIOPISTO

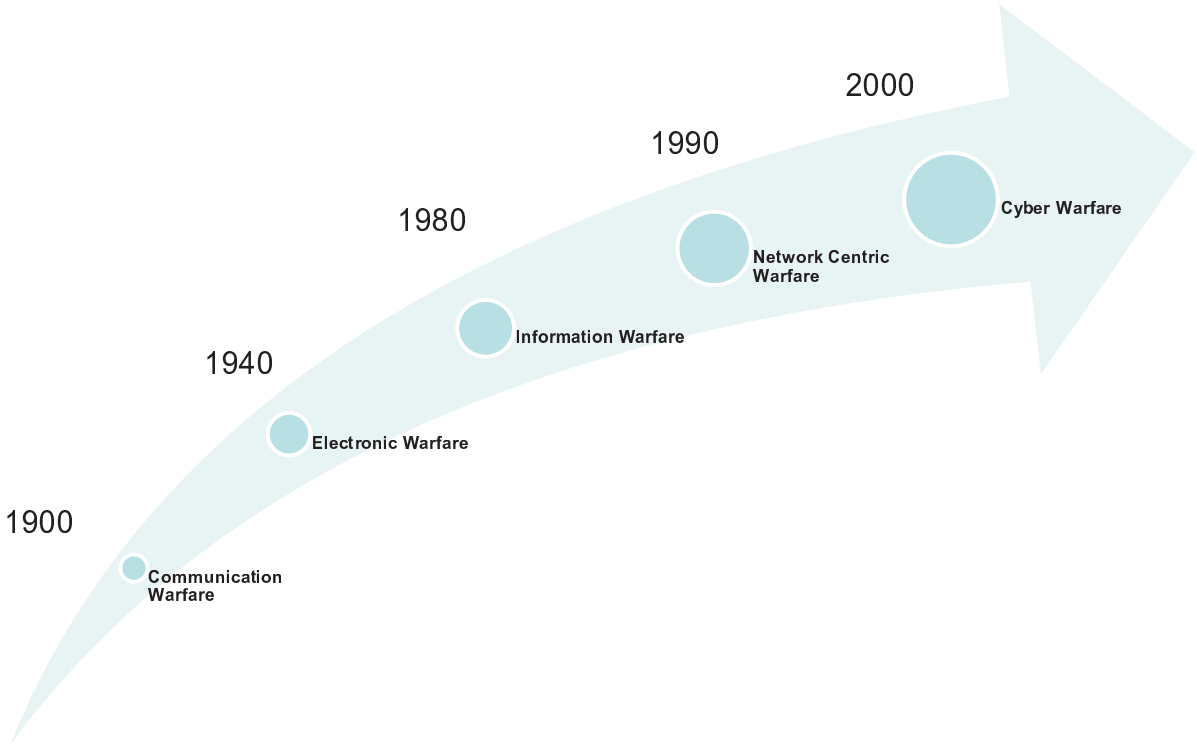
What is the **biggest threat to national cyber security?**



Defence IQ, How Confident Are We In Today's Cyber Defence Measures?, Aug 2012

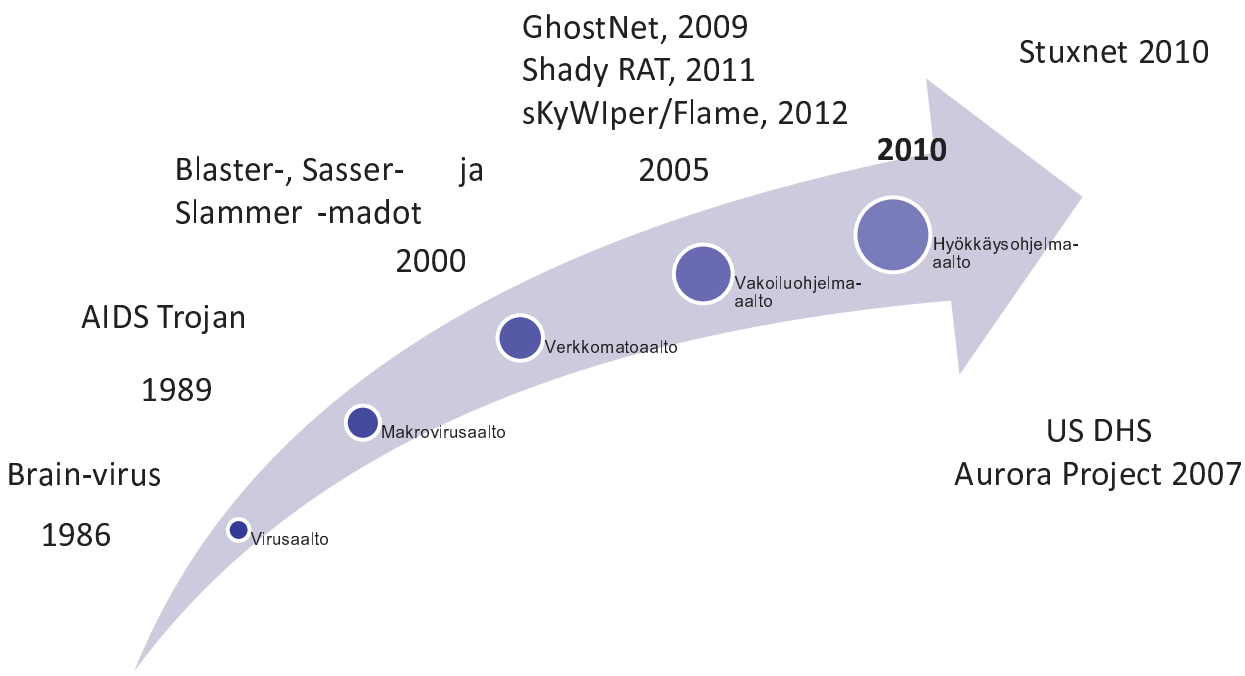
JYVÄSKYLÄN YLIOPISTO

Kybermaailman evoluutio



JYVÄSKYLÄN YLIOPISTO

Kyberaseiden evoluutio



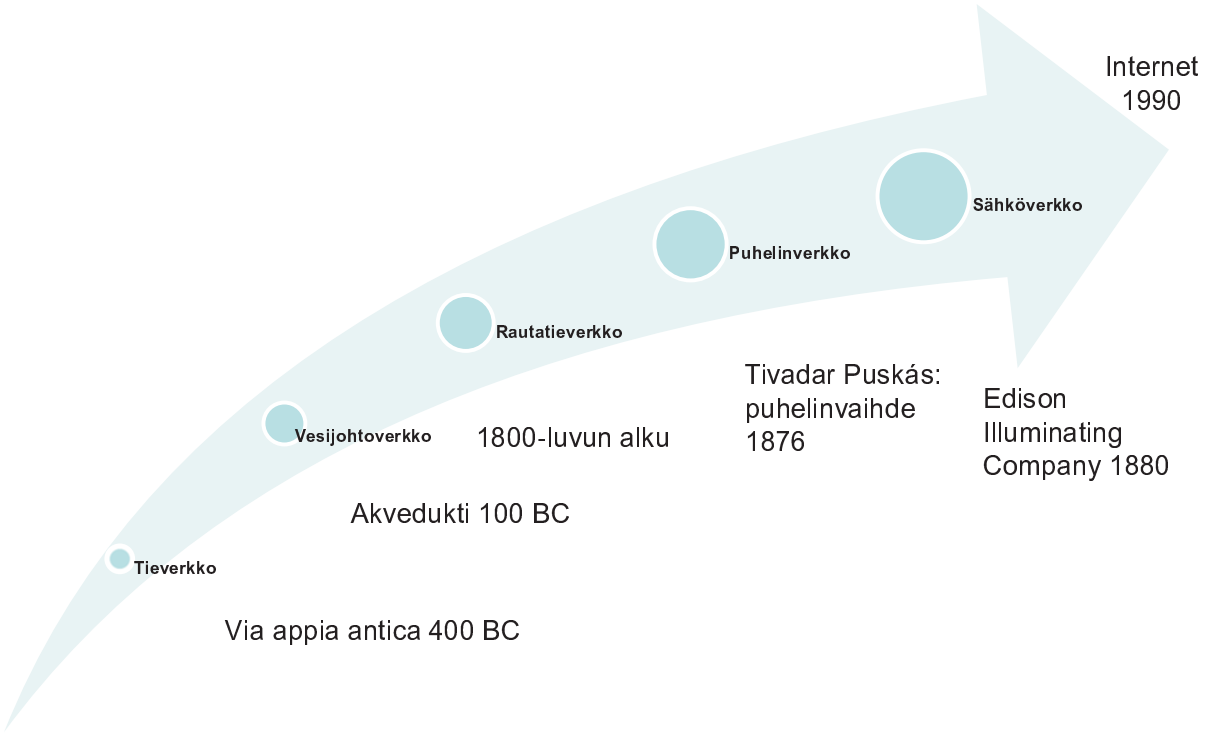
JYVÄSKYLÄN YLIOPISTO

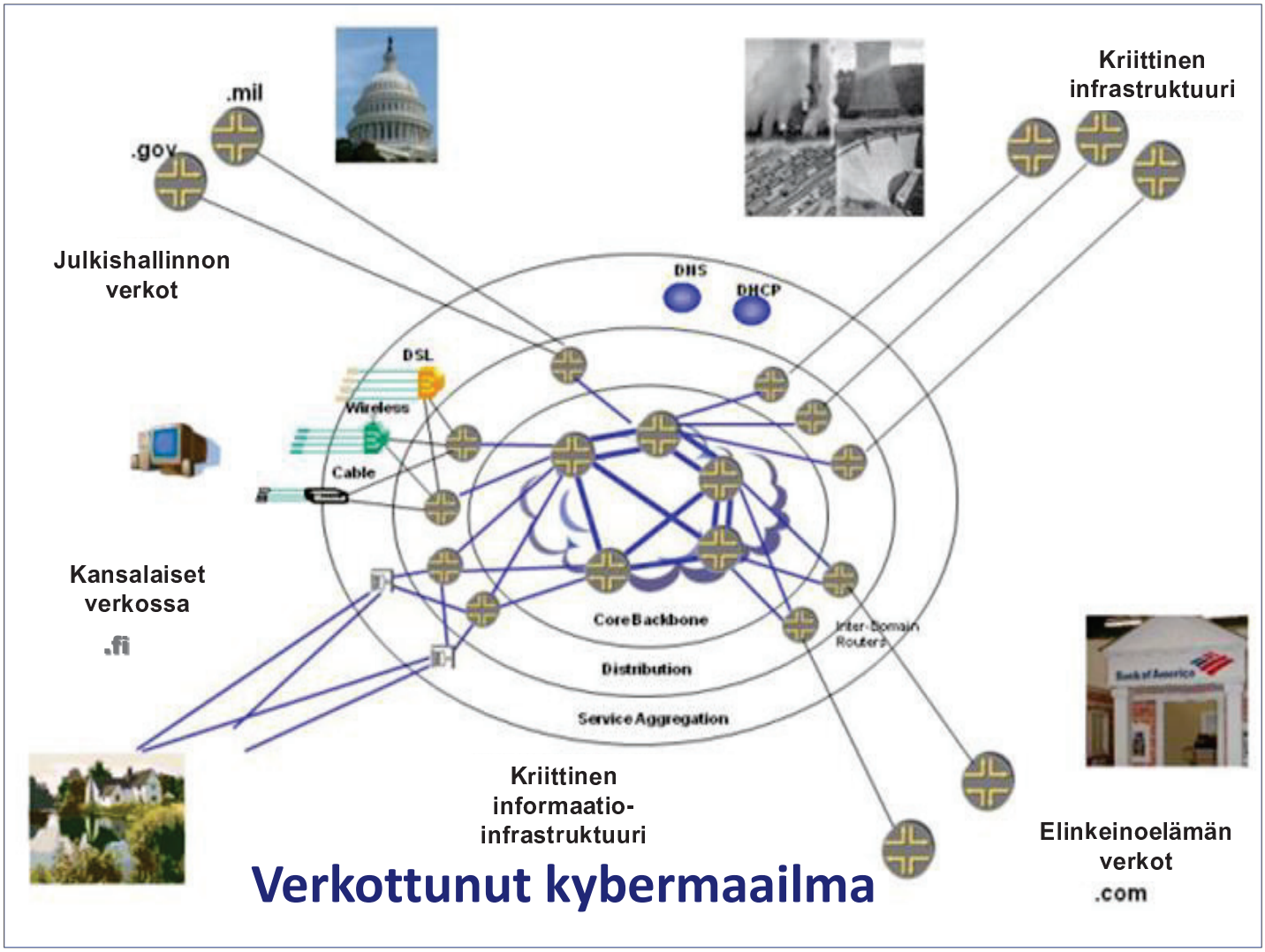
Voiko kybermaailmaa määritellä ja pitääkö sitä määritellä?

VERKOSTOT
ÄLYKKYYS
NOPEUS

JYVÄSKYLÄN YLIOPISTO

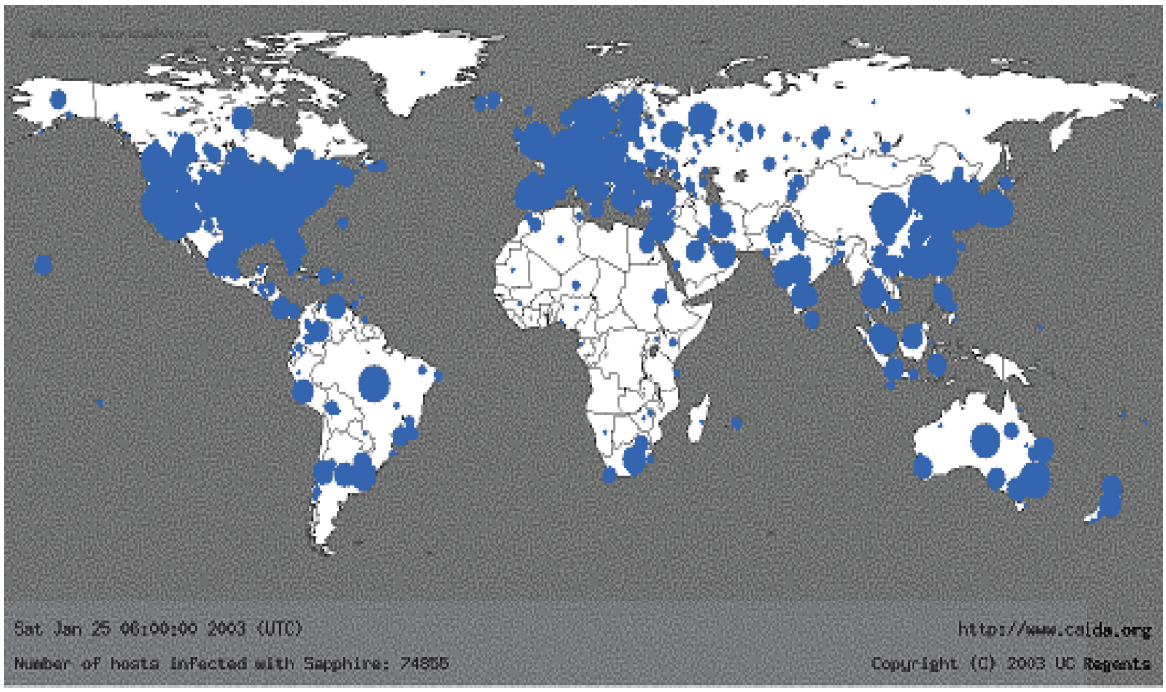
Verkostoevoluutio





JYVÄSKYLÄN YLIOPISTO

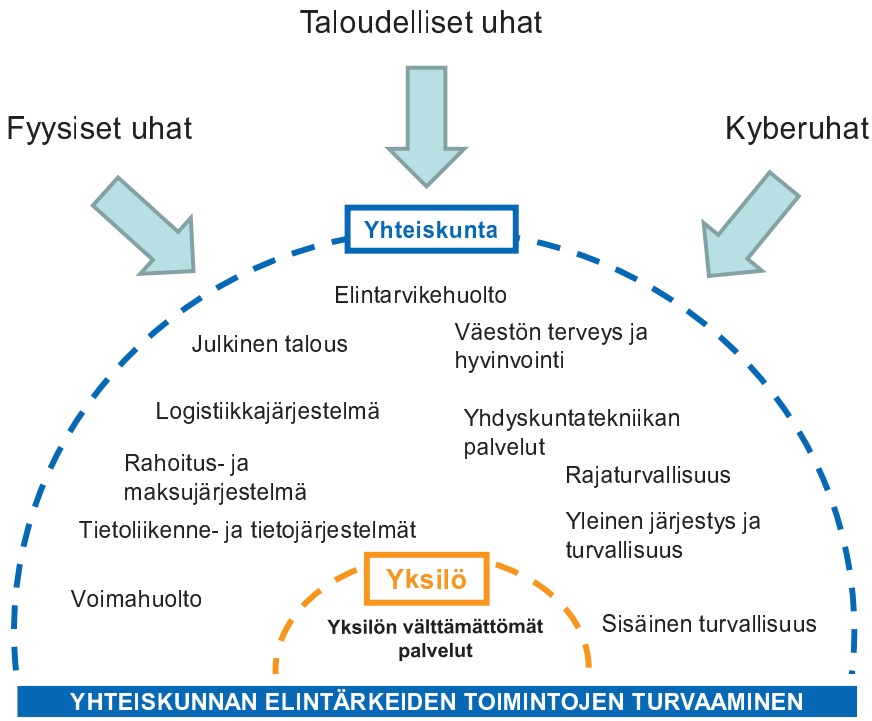
Ketterä kybermaailma



Slammer-madon levinneisyys 15 minuuttia hyökkäyksen aloittamisesta lauantaina 25.1.2003 05:30 UTC ; 75 000 saastunutta konetta

JYVÄSKYLÄN YLIOPISTO

Yhteiskunnan elintärkeät toiminnat ja niihin kohdistuvat uhat

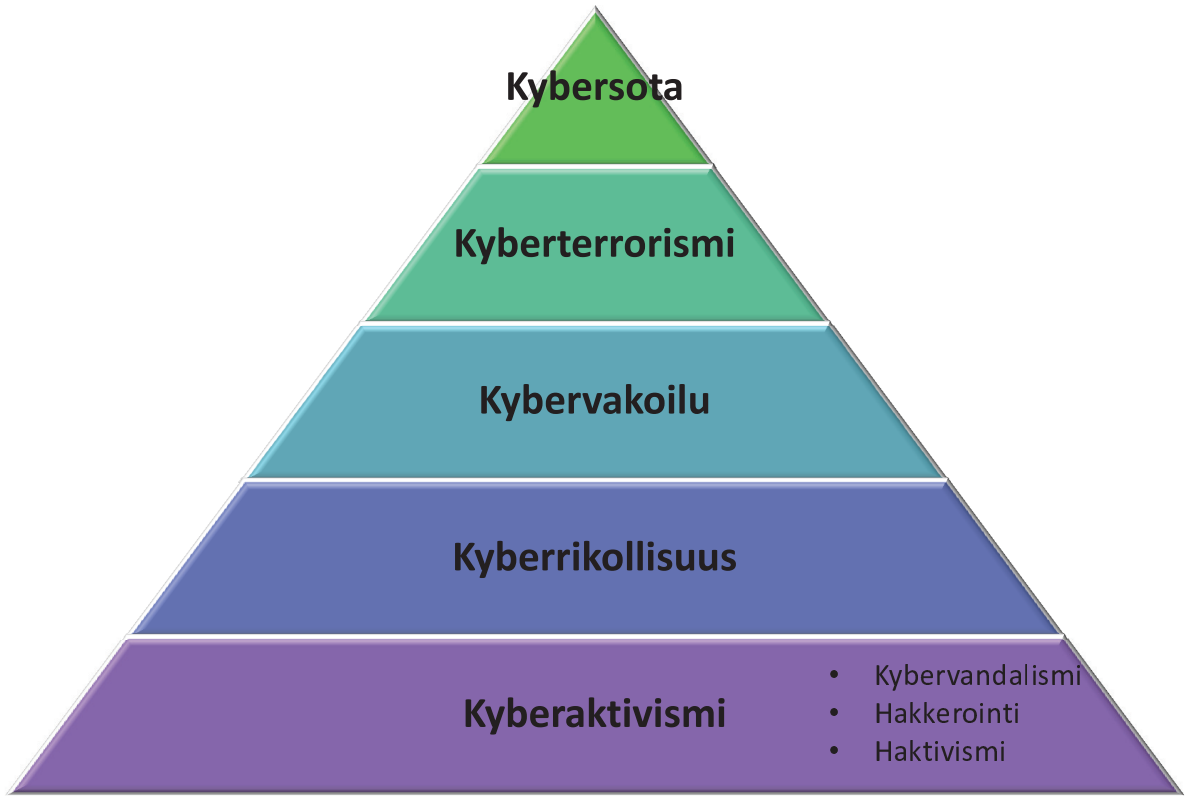


Fyysiset uhat: luonnon katastrofit, ympäristökatastrofit, perinteinen sota, terrorismi, kansalaistottelemattomuus

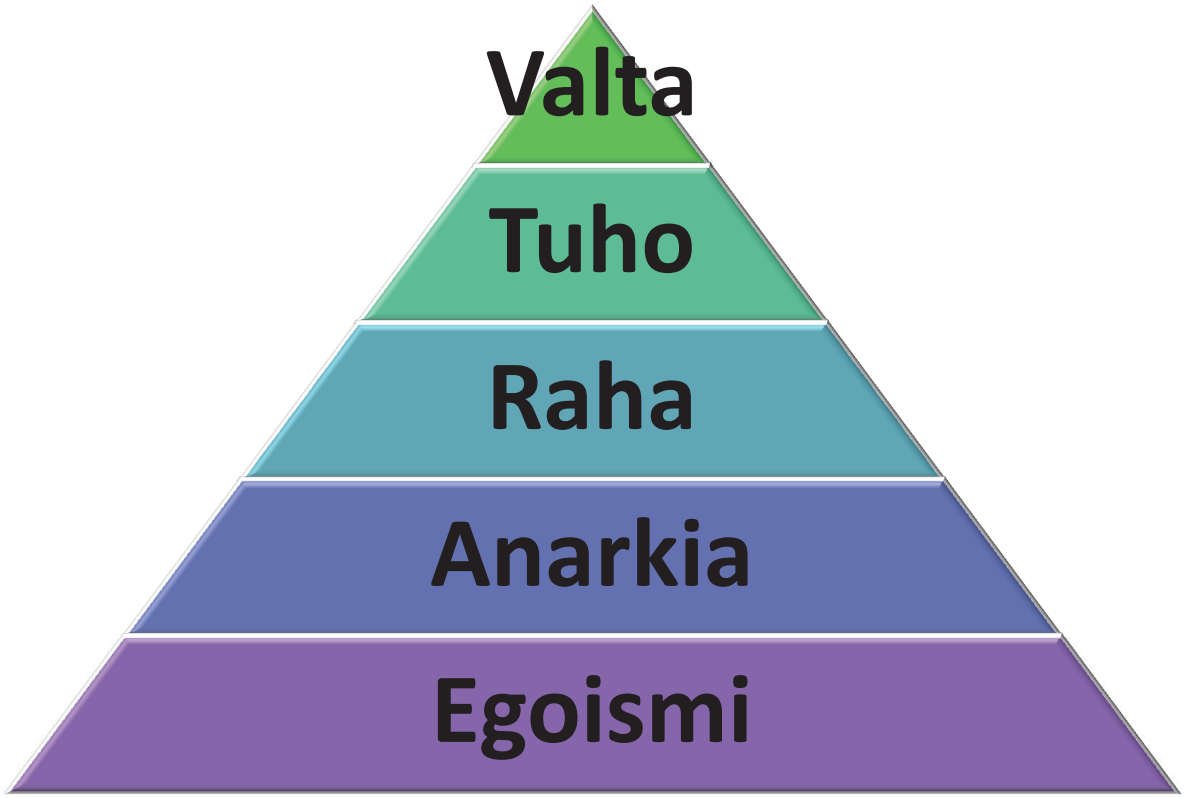
Taloudelliset uhat: kansantalouden romahdus, globaalin talouden romahdus

JYVÄSKYLÄN YLIOPISTO

Kyberuhkien rakenne toiminnan mukaan



Kyberuhkien rakenne motiivien mukaan



Kyberuhkien rakenne toimijoiden mukaan

Kybersodankäynti

"Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"

Richard A. Clarke, 2010

"Cyber war is hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence."

Joseph S. Nye Jr. 2011

"Refers to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems."

Myriam Dunn Cavelty, 2010

JYVÄSKYLÄN YLIOPISTO

USA kyberpuolustuskonsepti

1. Kyberdomain uutena ulottuvuutena
2. Kyberoperaatiokonsepti ml. aktiivinen kyberpuolustus
3. Yhteistyö Department of Homeland Security:n (DHS) ja yksityisen sektorin kanssa
4. Kollektiivisen kyberpuolustuksen rakentaminen
5. Kyberturvallisuusteknologian kehittäminen

US Cyber Command suunnittelee, koordinoi, integroi ja johtaa operaatioita ja puolustusta ja valmistautuu tarvittaessa johtamaan **täysimittaisia sotilaallisia kyberoperaatioita puolustusministeriön informaatioverkoissa**, jotta voidaan varmistaa Yhdysvaltojen ja sen liittolaisten toimintavapaus kyberavaruudessa ja kiistää sen käyttö vastustajilta.

Venäjän kyberpuolustuskonsepti

Konfliktin eskaloituminen kyberavaruuteen ja muuttuminen kriisiksi antaa oikeuden omaan tai kollektiiviseen itsepuolustukseen hyväksikäyttäen kaikkia tarpeellisia keinoja, jotka eivät ole ristiriidassa hyväksyttyjen normien ja kansainvälisten sopimusten kanssa.

Kyberhyökkäysten torjunnassa konsepti sisältää ajatuksen kyberturvallisuusjoukoista toisen valtion alueella. Tällaisten joukkojen sijoittaminen voi perustua vapaaehtoisuuteen tai kansainvälisen oikeuden suomaan mahdollisuuteen.

Kybersotaa voidaan torjua myös muiden sodankäynnin keinoin.

JYVÄSKYLÄN YLIOPISTO

Kiinan kyberpuolustuskonsepti

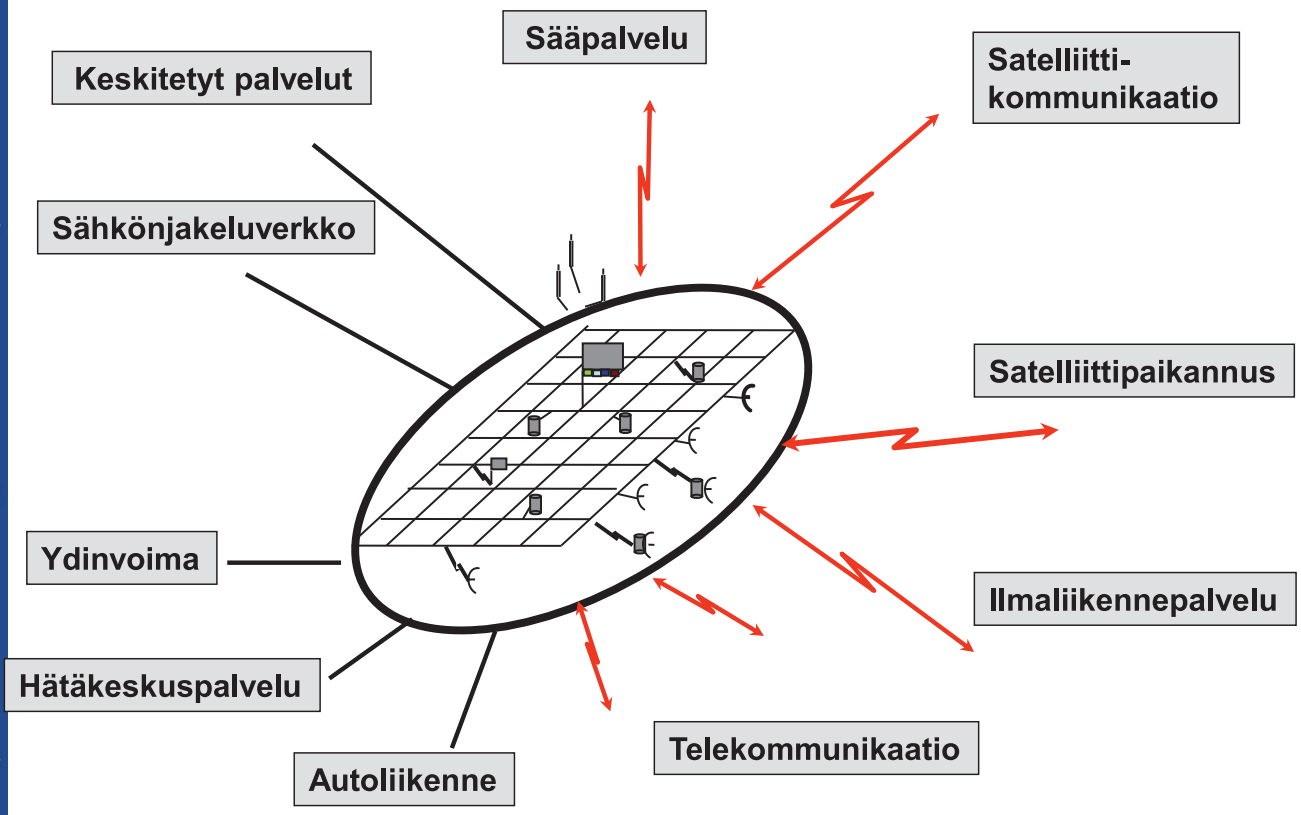
Kiinan kyberpuolustusstrategia ilmentyy vuonna 2009 julkaistussa strategiassa: “**Integroitu verkkokeskeinen elektroninen sodankäynti**” (wangdian yitizhan)

Strategiassa on kysymys elso- ja tietoverkko-operaatioiden samanaikaisesta käyttämisestä vastustajan elintärkeitä TVJ- ja muita informaatiojärjestelmiä vastaan. Strategian mukaan verkkohyökkäystyökaluja käytettäisiin **konfliktien alkuvaiheessa ja mahdollisesti ennaltaehkäisevästi.**

Tavoitteena on toteuttaa **lamauttavia iskuja** johtamisjärjestelmään samalla kun käytetään ohjuksia , ilmahyökkäyksiä ja erikoisjoukkojen iskuja fyysisiin kohteisiin ja laitteisiin.

JYVÄSKYLÄN YLIOPISTO

Uusia uhkia kybersodassa?



JYVÄSKYLÄN YLIOPISTO

Kyberturvallisuus ja osaaminen

Nykyisen hallitusohjelman mukaan kansallisen kyberturvallisuuden tavoitteena on, että ”Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä”.

Kustannustehokkain tapa lisätä kansallista kyberturvallisuutta on osaamisen parantaminen.

Kyberturvallisuuden opetuksen yleisenä tavoitteena tulisi olla kansalaisten, viranomaisten ja elinkeinoelämän toimijoiden tietoisuuden lisääminen kybertoimintaympäristön uhkista ja riskeistä sekä kaikkien osaamisen parantaminen kyberturvallisuustoimenpiteitä toteutettaessa.

Alan huippututkimuksella luodaan perusta sekä osaamisen että kyberturvallisuusjärjestelmien kehittämiselle.

JYVÄSKYLÄN YLIOPISTO

Kyberturvallisuus ja osaaminen

Tavoitteita:

Nykyistä kyberturvallisuuden tutkimuksen tasoa tulee nostaa ja turvata tutkimusedellytykset, jotta kyetään jatkuvasti tuottamaan sekä perustutkimuksella että soveltavalla tutkimuksella korkeatasoisia uusia innovaatioita ja tieteellisiä läpimurtoja.

Tämä edellyttää kansallista lisäpanostusta kybertutkimukseen.

Kyberturvallisuuden strateginen huippuosaamisen keskittymä (KYBER-SHOK) tarjoaisi huipputason tutkimusyksiköille ja tutkimustuloksia hyödyntäville yrityksille tehokkaan tavan tehdä tiivistä ja pitkäjänteistä yhteistyötä keskenään.

JYVÄSKYLÄN YLIOPISTO

Informaatioturvallisuuden koulutuksen tavoite

Jyväskylän yliopiston informaatioturvallisuuden opintokokonaisuuden koulutuksen tavoitteena lukuvuonna 2012–2013 on antaa opiskelijalle johdatus kyberturvallisuuden kokonaisuuteen informaatioturvallisuuden yhteiskunnallisen ja teknologisen sekä kybermaailman turvallisuuden ja turvallisuusjohtamisen näkökulmien perusteella.

Opintotarjontaa on yhteensä 39 opintopistettä.

Tiedolliset ja taidolliset erityistavoitteet

Informaatioturvallisuuteen suuntautunut maisteri kykenee määrittelemään tietoon, tietoverkkoihin, -liikenteeseen ja järjestelmiin sekä toimintaprosesseihin liittyviä informaatioturvallisuusriskejä.

Hänellä on hyvät valmiudet suunnitella, toimeenpanna ja toteuttaa järjestelmien ja organisaatioiden informaatioturvallisuusstrategioita.

Hän kykenee soveltamaan uusimpia teknologioita tietoturvallisuusongelmiin ja tuottamaan ajantasaisia suunnitelmia ja ratkaisuja.

JYVÄSKYLÄN YLIOPISTO

Tiedolliset ja taidolliset erityistavoitteet

Kurssien ja tutkimustyön erilaisilla valinnoilla opiskelija voi suuntautua erilaisiin työtehtäviin kuten:

- **Oman organisaation turvaaminen** (turvallisuuspäällikkö, turvallisuusasiantuntija)
- **Järjestelmäkehitys** (turvallisuusohjelmistojen ja tietojärjestelmien kehittäjä)
- **Tuotekehitys** (turvallisuustuotteiden kehittäjä)
- **Turvallisuustuotteiden ja -menetelmien myynti ja markkinointi** (turvallisuusasiantuntija)

JYVÄSKYLÄN YLIOPISTO

Kurssitarjonta 2012-13

Lukuvuonna 2012–2013 informaatioturvallisuuden kurssitarjonta muodostuu kahdeksasta kurssista:

ITKST40 Yhteiskunta ja informaatioturvallisuus, 5 op
- Professori Rauno Kuusisto

ITKST41 Kybermaailma ja turvallisuus, 5 op
- Tutkija, ST Martti Lehto

ITKST42 Information Security Technology , 5 op
- PhD Gil David

ITKST43 Informaatioturvallisuuden johtaminen, 5 op
- Professori Rauno Kuusisto

ITKST44 Kybermaailma ja kansainvälinen oikeus, 4 op
- Tutkija Kari Takanen

ITKST45 Introduction to cyber conflict, 5 op
- PhD Rain Ottis

ITKST46 Cyber security management, 5 op
- PhD Rain Ottis

ITKST47 Advanced Anomaly Detection: Theory, Algorithms and Applications, 5 op
- PhD Gil David

JYVÄSKYLÄN YLIOPISTO

Muu informaatioturvallisuuden kurssitarjonta

Enterprise Level Security, TJTSS73, 3 op
- PhD Dipankar Dasguptan, University of Memphis

Tietoturva, TIES326, 5 op
- Professori Timo Hämäläinen

Oppilaitosturvallisuus, koulutusteknologian tietoturva ja yksityisyys, koulujen tietoturvakulttuuri, TIES466, 5 op
- tutkimusjohtaja Hannakaisa Isomäki

JYVÄSKYLÄN YLIOPISTO

Kyberturvallisuuden tutkimus- ja koulutuskenttä

Kyberjuridiikka

Kyberturvallisuuden integrointi

Kyberturval-lisuuskoulutus

Kyberturvallisuuden liiketoiminta

Kyberturvallisuuden hallinta ja johtaminen

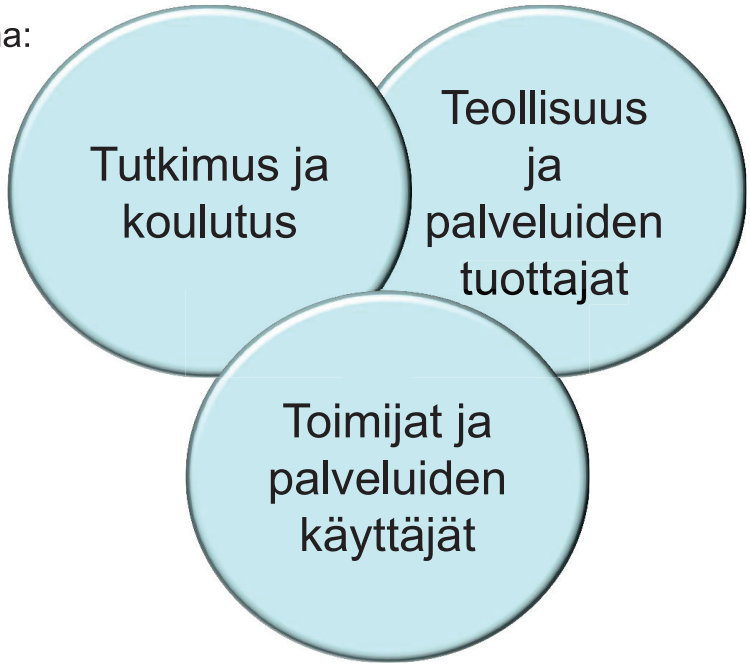
Kyberturvallisuus-teknologia

JYVÄSKYLÄN YLIOPISTO

Kyberturvallisuuden yhteistoiminnan haasteet

Kilpailuasetelma:
- rahoitus

Kilpailuasetelma:
- business



Kilpailuasetelma:
- johtajuus

Kyberturvallisuuden tasapaino

Technology factor

- Tehokkaampia palomuureja
- Kehittyneempää haittaohjelmatorjuntaa
- Tehokkaampaa salausta

Human factor

- Johtajuus
- Osaaminen
- Kulttuuri
- Prosessit

Varautumisen haaste

Pearl Harbor 1941	→	Yhdysvallat liittyi sotaan ja varustautuminen alkoi
Terroristihyökkäys 11.9.2001	→	Terrorismin vastainen sota ja suojautuminen
Aasian tsunami 2004	→	Suojautumisen tehostaminen Tsunamivaroitusjärjestelmä
Hurrikaani Katrina 2005	→	Suojautumisen tehostaminen Ennakkovaroituksen tehostaminen

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Jyvsectec – turvallisuusteknologian kehittämishanke

Marko Vatanen, Asiantuntija, JYVSECTEC-projekti, Jyväskylän ammattikorkeakoulu

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Euroopan unioni
Euroopan aluekehitysrahasto

Vipuvoimaa EU:lta 2007–2013

JYVSECTEC

Jyväskylä Security Technology

Kyberturvallisuus seminaari, Tampere 6.9.2012

Marko Vatanen, Asiantuntija, JYVSECTEC-projekti

CASSIDIAN AN EADS COMPANY AJECO descom Relator JYKES Success together.

Euroopan unioni
Euroopan aluekehitysrahasto

Vipuvoimaa EU:lta 2007–2013

JYVSECTEC 2,4 MEUR

- JYVSECTEC (Jyväskylä Security Technology) on turvallisuusteknologian kehittämisprojekti
- Projektin julkisina osarahoittajina toimivat Keski-Suomen Liitto ja Euroopan aluekehitysrahasto
  - EU:n ja valtion tuki 59% (1,4 MEUR)
- Projekti käynnistyi syyskuussa 2011 ja jatkuu vuoden 2013 loppuun
- JYVSECTEC:ssä luodaan Keski-Suomeen turvallisuusalan yritysten ja toimijoiden yhteistyöverkosto
- Tavoite olla yksi Suomen johtavista kyberturvallisuuden kehittämis- ja koulutuskeskus

Projektin osapuolet

- **Projektin toteuttaja:**
  - Jyväskylän AMK:n teknologiayksikön ICT-tulosalue
- **Projektin yhteistyökumppaneina:**
  - Cassidian Finland Oy
  - Descom Oy
  - Relator Oy
  - Ajeco Oy
  - Jyväskylän seudun kehittämisyhtiö Jykes Oy

Projektin sopimuskumppanit

- Projektin infrastruktuurin puitesopimuskumppanina toimii TeliaSonera Finland Oyj / Cygate Oy
- Projektin TETRA-verkkoympäristön toimittajana on Cassidian Finland Oy
- Tietoturvaratkaisut ja tilannekeskusratkaisut tullaan kilpailuttamaan tarpeen mukaan

Projektin tavoitteet

- **Suunnitella ja rakentaa kyberturvallisuuden kehitys-, testaus- ja koulutusympäristö sisältäen**
  - Laitteistot ja ohjelmistot
  - Palvelut asiakkaille ja käyttäjille
  - Tilannekeskus, jossa voidaan esittää erilaisia tilannekuvia
- **Osaamiskeskuksen toiminta**
  - Kansallisten/kansainvälisten yhteistyömahdollisuuksien tunnistaminen ja kehittäminen
  - Tietoisuuden lisääminen Keski-Suomen tarjoamista kehitysympäristömahdollisuuksista
  - Verkostoitumismahdollisuus kansainvälisille toimijoilla ja yhteistyöyrityksille

Kehitysympäristön toimintamuotoja

- **Mahdollisuus toteuttaa todellisia tilanteita realistisessa, mutta suljetussa ympäristössä**
  - Mahdollistaa yritysten ja heidän asiakkaidensa testata tuotteitaan halutussa ympäristössä (esim. uhkaskenaariot, kyberharjoitukset)
  - Tuotekehitys suljetussa ja realistisessa ympäristössä
  - ”Hands-on” koulutus/harjoittelu eri toimijoiden kanssa
- **Testataan ja arvioidaan uusien kehitteillä olevien ratkaisujen toimivuutta puolueettomasta näkökulmasta**
  - Keskitetyt kyberturvallisuuden testaus ja asiantuntijapalvelut
  - Teknisen ratkaisun soveltuvuuden arviointi vertailutesteillä
  - Kyberturvallisuuden tilannekuvan muodostaminen
- **Tilannekeskuksen toiminta palveluiden tuottamisessa**
  - Tilannekuvan muodostaminen eri tasoille, mm. tietoturvan tekninen tilannekuva, tietoturvan hallinnollinen tilannekuva

Kyberharjoitus

- JYVSECTEC valmistelee osana projektia kyberharjoitusta, jossa eri toimijat voivat harjoitella mahdollisimman realistisessa ympäristössä toimintaa erilaisia verkosta tulevia kyberuhkia vastaan
- Ensimmäinen ulkopuolisia osallistujia sisältävä harjoitus/koulutustapahtuma järjestetään keväällä 2013
- Kiinnostuneet tahot voivat ottaa yhteyttä projektin yhteyshenkilöihin
- Lisäksi kyberharjoitus tullaan toteuttamaan osana Ylemmän AMK-tutkinnon ”loppusotaa” vuonna 2014

JYVSECTEC-liiketoiminta vuonna 2014

- **Toimintaympäristö ja tilannekeskus on otettu käyttöön**
- **Pilotoidut koulutus-, testaus- ja tuotekehityspalvelut on otettu käyttöön**
- **Yhteistyöverkoston liiketoimintamalli on muodostettu**
- **Kyberturvallisuutta hyödyntävien toimijoiden välisiä alueellisia ja kansainvälisiä yhteistyömuotoja on otettu käyttöön**
  - Puolueeton keskus/foorumi avoimelle tiedonvaihdolle/jakamiselle
  - Kansainvälinen yhteistyö on edennyt
- **Turvallisuusalan kansainvälisten toimijoiden tietoisuus Keski-Suomen tarjoamista kehitysympäristömahdollisuuksista on lisääntynyt**
  - Uusien kansainvälisten tutkimushankkeiden valmisteluja on käynnistetty

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Euroopan unioni
Euroopan aluekehitysrahasto

Vipuvoimaa EU:lta 2007–2013

KYSYMYKSIÄ?

CASSIDIAN AJECO descom Relator JYKES Success together.

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Euroopan unioni
Euroopan aluekehitysrahasto

Vipuvoimaa EU:lta 2007–2013

Yhteystiedot

Jarmo Siltanen, Koulutus- ja T&K-päällikkö
Email: jarmo.siltanen@jamk.fi
GSM: +358 40 716 7282
Petteri Weckström, projektipäällikkö
Email: petteri.weckstrom@jamk.fi
GSM: +358 40 531 3239
Jari Hautamäki, Yliopettaja
Email: jari.hautamaki@jamk.fi
GSM: +358 40 540 2361
Marko Vatanen, Asiantuntija
Email: marko.vatanen@jamk.fi
GSM: +358 40 545 8630

CASSIDIAN AJECO descom Relator JYKES Success together.

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Cognitive Networks and Cyber Threats

Anssi Kärkkäinen, Kapt., Defence Command Finland

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

Cognitive Networks and Cyber Threats

Anssi Kärkkäinen
Defence Command Finland

Kyberturvallisuusseminaari
6.9.2012

Introduction

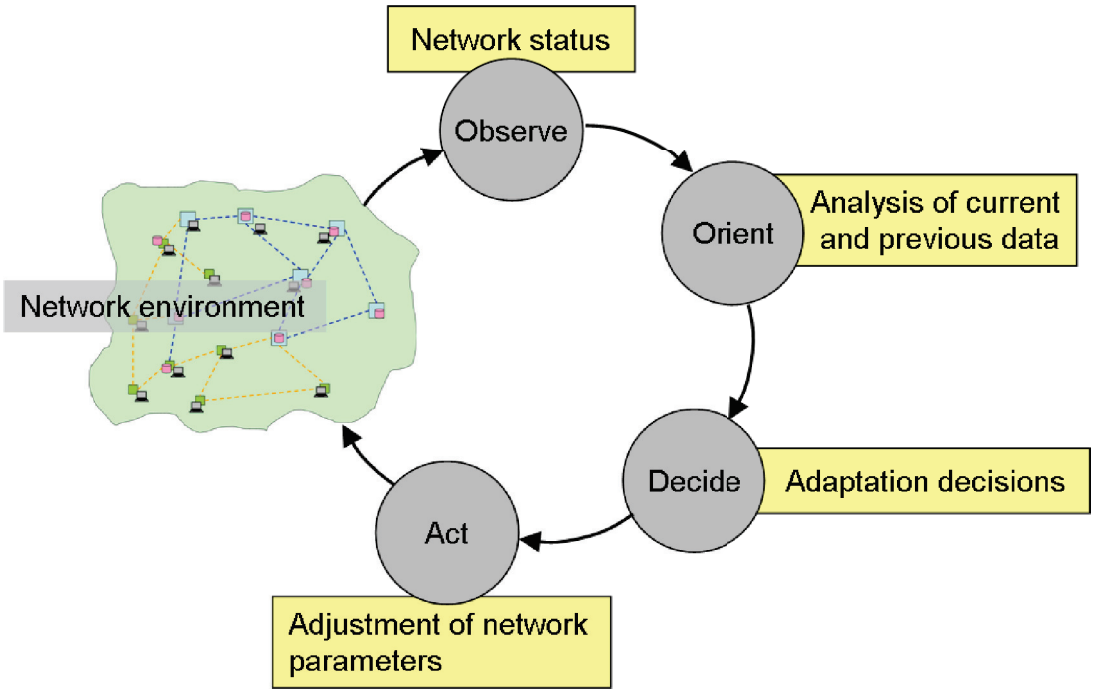
- Next generation networks are Cognitive Networks (CN)?
  - Resource management (spectrum etc.)
  - Interoperarbility
  - Self-orientation
- Benefits in military environments
  - Fast configuration (no man-in-the-loop)
  - Better security?
  - Resource usage
- Cyber threats are incraesing
  - CN leads to new threats?

PUOLUSTUSVOIMAT | FÖRSVARSMAKTEN | THE FINNISH DEFENCE FORCES

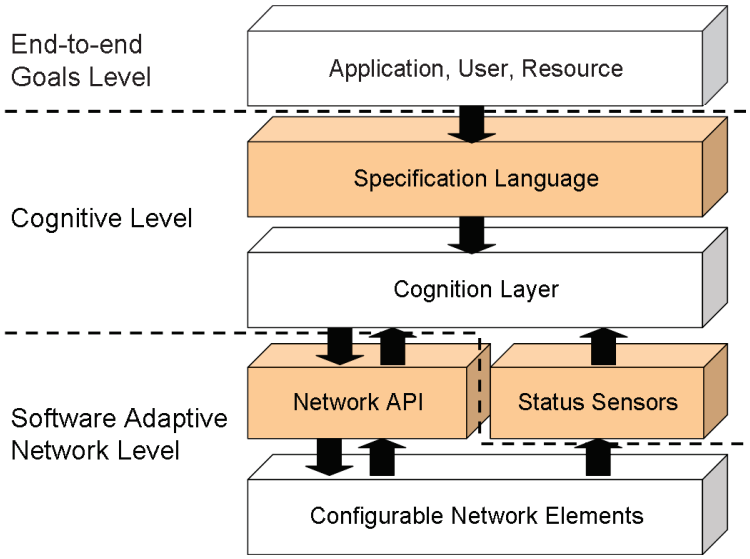
Cognitive Networks

”A cognitive network is a network with a cognitive process that can perceive current network conditions, and then plan, decide, and act on those conditions. The network can learn from these adaptations and use them to make future decisions, all while taking into account end-to-end goals.”

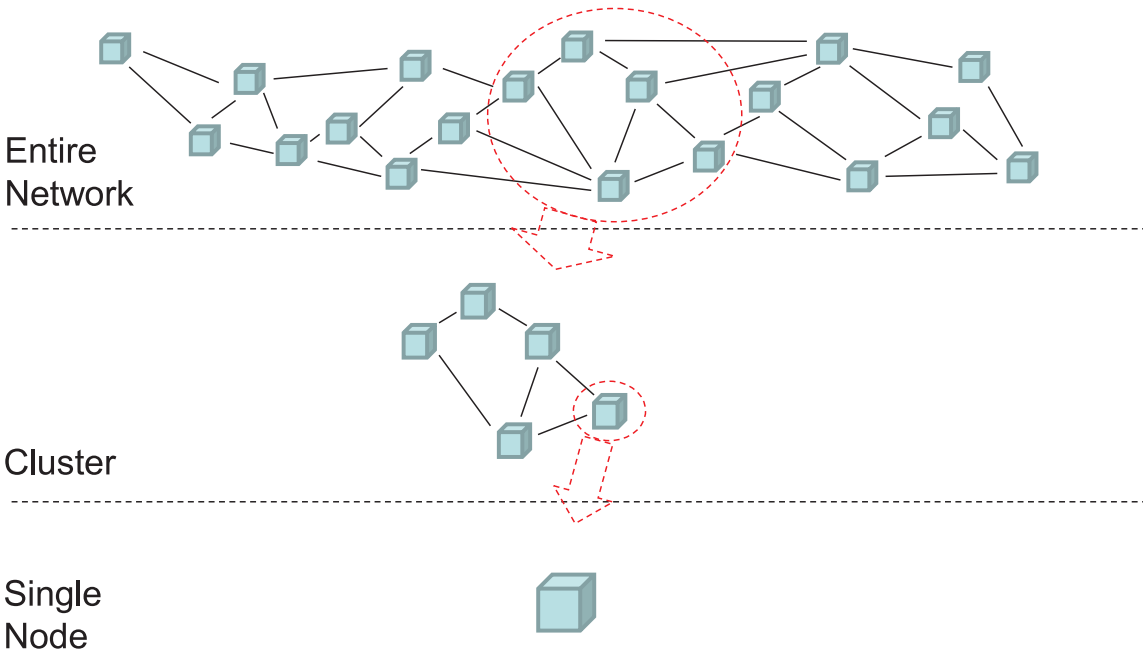
Cognitive Networks



Cognitive System Framework



Layered Optimizing



Elements for Cognitive Process

- Decision-making and learning algorithms
- Optimization processes and methods
- Information sharing between and inside nodes
- Databases to store history and previous data
- Sensors to provide input data
- Software defined hardware

Security Goals

– Confidentiality
– Integrity
– Availability
– Access control
– Authentication
– Non-repudiation
– Communication security
– Privacy

About Cyber Threats

- Global playground
- Number of sources:
  - National Governments
  - Terrorists
  - Industrial Spies and Organized Crime Groups
  - Hacktivists
  - Hackers
- Number of targets
  - Banking and Finance
  - Commercial Facilities
  - Communications and Information Technology
  - Critical Manufacturing, Emergency Services, Healthcare and Public Health
  - Energy and Nuclear Reactors
  - Transportation, Postal and Shipping, Water Systems
- Small resources, high possibilities

Cyber Attacks…

Sophisticated botnet command and control attacks

GUI intrusion tools

Widespread, distributed denial-of-service attacks

Widespread attacks using NNTP to distribute attack

Targeting of specific users

Packet spoofing

Analysis of vulnerabilities in compiled software without source code

Wide-scale use of worms

Windows-based remote access trojans (Back Orifice)

Distributed attack tools

1. **Penetration Attacks** – Espionage, data modification, manipulation
2. **Denial-of-Service Attacks**

Executable code attacks

"Stealth" and other advanced scanning techniques

Automated widespread attacks

Automated probes and scans

Widespread attacks on DNS infrastructure

Cyber-threats & bullying (not illegal in all jurisdictions)

Email propagation of malicious code

Wide-scale trojan distribution

Anti-forensic techniques

Industrial espionage

Network sniffers

Session-hijacking

Internet social engineering attacks

Offensive Cyber Operations

Examples of the desired effects:

- bandwidth reduction
- information compromise
- information uncertainty
- unavailability of information
- loss of communications

New Targets for Cyber Attacks

Threat	Description	Implication
Sensor Input Violation	Sensory input data is altered by an attacker or other means	Decisions are made according to false situation awareness which can result in faulty performance.
Information Sharing Violation	Information sharing between network nodes is damaged	Situation awareness of surrounding environment is false. Decisions are made according to false information which can result in faulty performance.
Data Storage Attack	Knowledge data storages in network nodes are injured.	Previous data may be incorrect which causes a risk of imperfect decisions.

CN Specific Cyber Attacks

Physical Layer

- Control Channel Jamming Attack
- Primary Receiver Jamming Attack
- Overlapping Other Users Attack
- Node capture

Link Layer

- Biased Utility Attack
- Asynchronous Sensing Attack
- False Feedback Attack

Network Layer

- Network/Channel Parasite Attack
- Misleading Information Attack

Transport Layer

- TCP/UDP Attacks

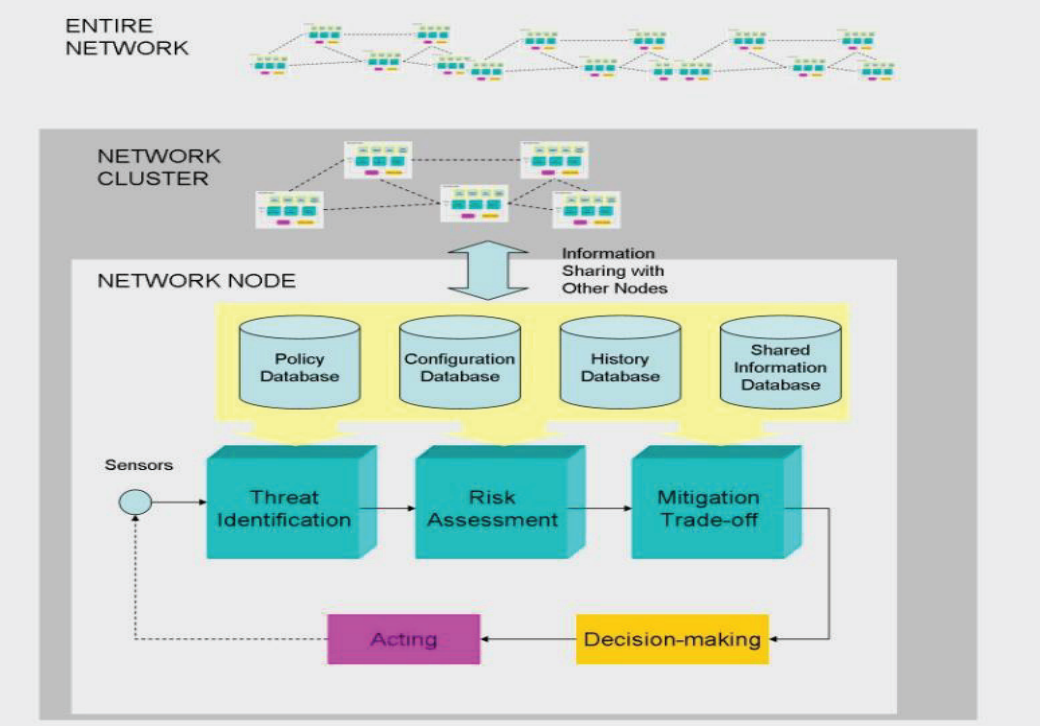
Application Layer

- Selfish Misbehavior – concealing available resources from other nodes

Cross-layer

- Jellyfish Attack
- Routing Information Jamming Attack

A Threat Management Model



PUOLUSTUSVOIMAT | FÖRSVARSMAKTEN | THE FINNISH DEFENCE FORCES

Challenges with CNs

- Implementing security features into a cognitive process
- Control channel protection
- Detection of misbehavior
- Updating threat databases

Conclusion

- Cognitive networking will provide smart functionalities for future military communication networks
  - Flexible resource usage, less human configuring and management and more security? features
- CN provides new targets for cyber attackers
  - Control channels
  - Sensors
  - Cognitive process
  - Databases
- Implementing security features is challenging
  - Automated decision-making process
  - Distributed control and optimizing (in a military environment)

References

- Clancy, T.C. and Goergen, N. (2008) "*Security in cognitive radio networks: threats and mitigation*", **3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications** (CrownCom), pp 1 - 8.
- Fragkiadakis, A., Tragos, E. and Askoxylakis, I. (2012) "*A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks*", **IEEE Communications Surveys & Tutorials**, Vol PP, *Issue 99, pp 1 – 18.*
- *Mahmoud, Q. (2007), "Cognitive Networks: Towards Self-Aware Networks", Wiley-Interscience, 2007.*
- Mody et all (2009) "*Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard*", **IEEE Military Communications Conference** (MILCOM), pp 1 - 7.
- Prasad, N. (2008) "*Secure cognitive networks*", **European Conference on Wireless Technology**, pp 107 – 110.
- Thomas, R., DaSilva, L. and MacKenzie, A. (2005) "*Cognitive networks*", **Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks**, pp 352 – 360.
- Ventre, D., "*Cyberwar and Information Warfare*", **John Wiley & Sons, Inc.**, 2011.
- Anssi **Kärkkäinen**, "C*yber Threat Management in Cognitive Networks",* 11th European Conference on Information Warfare and Security, 2012.
- Fragkiadakis A., Tragos E. and AskoxylakisI. "*A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks*", IEEE Communications Surveys & Tutorials, Volume: PP , Issue: 99, Page(s): 1 – 18, 2012.

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Tietoverkkorikollisuus – haaste poliisille ja yhteiskuntatieteelliselle tutkimukselle

Anna Leppänen, Tutkija, Poliisiammattikorkeakoulu, tohtorikoulutettava, Tampereen yliopisto

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

Tietoverkkorikollisuus –
haaste poliisille ja yhteiskuntatieteelliselle tutkimukselle

Kyberturvallisuus, hyökkäys ja puolustus –seminaari 6.9.2012

Anna Leppänen
Tutkija
Poliisiammattikorkeakoulu
Tampereen yliopisto, turvallisuushallinnon tohtorikoulutettava

Esityksen rakenne

- Tietoverkkorikoksen määritelmiä
- Rikollisuuden luonne vs. poliisitoiminnan perinteet
- Poliisin tilastoja
- Yhteiskuntatieteellisiä aineistonkeruutapoja ja niiden rajoituksia tietoverkkorikollisuuden tutkimuksessa
- Tietoverkkorikostutkinnan toimintaympäristö, organisointi ja viranomaisyhteistyö (alkava turvallisuushallinnon väitöstutkimukseni)

Tietoverkkorikoksen määritelmiä

- Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hengessä
  - Rikos, joka kohdistuu tietojärjestelmään tai tehdään tietoverkon avulla
  - Tietotekniikkarikos ja tietoverkkorikos samoja asioita
- Poliisin sisällä tietotekniikkarikosta on ehdotettu sateenvarjokäsitteeksi
  - Tietoverkkorikokset (hakkerointi, palvelunestohyökkäykset, haittaohjelmat ym.)
  - Tietoverkkoja hyväksikäyttäen tehtävät rikokset (ns. internet-petokset, laiton tietosisältö, maksuvälinepetokset verkossa, kunnianloukkaukset ym.)
  - Tietotekniikkaa hyväksikäyttäen tehtävät rikokset (esim. paikallisessa tietojärjestelmässä tehdyt petokset ja kavallukset)

Tietoverkkorikollisuuden luonne

- Motiiveina esim. taloudellisen hyödyn tavoittelu, haktivismi, valtiolliset motiivit, hauskanpito
- Rikolliset kapean alan asiantuntijoita: haittaohjelman kirjoittajat, levittäjät, hallinnoijat ja rahastajat eri henkilöitä
- Myyvät ja ostavat tietoa verkossa erilaisilla foorumeilla
- Eivät yleensä tunne toisiaan kuin verkossa
- Haittaohjelma piiloutuu uhrilta -> vrt. 2000-luvun alku
- Yksittäinen tapaus on usein pieni sirpale kokonaisuudesta ja uhri ei välttämättä edes tiedä olevansa uhri
- Rikollisen tarvitsee löytää yksi aukko, puolustuksen pitäisi tukkia kaikki

Tietoverkkorikollisuuden haaste poliisille

- On syntynyt uusi globaalin rikollisuuden ulottuvuus, joka ulottuu perinteisen, paikkaan sidotun poliisitoiminnan ulkopuolelle
- Tapaukset koostuvat monista teoista -> sirpalemaisuus vääristää
- Rikosepäilyt vaativat tiivistä ja nopeaa kansallista ja kv-yhteistyötä (uhrit, tekijät, ”tekovälineet”, rahastus eri maissa/vähintään eri puolilla valtioita)
- Yhteistyötä niin viranomaisten kuin yksityisen sektorin välillä
- Erilaiset lainsäädännöt, osaamisen puute, resurssipula ongelmina
- Jatkuva kehitys
- Rikosepäilyistä ei ilmoiteta poliisille -> yritykset pelkäävät maineensa puolesta, eivät usko poliisin selvittävän rikosta

6.9.2012

Poliisin tilastoja: tietotekniikkarikokset

Vuosi	KRP	Paikallispoliisi	Yhteensä
2012	58	848	**906**
2011	34	332	**366**
2010	38	272	**310**
2009	21	279	**300**
2008	15	436	**451**
2007	33	501	**534**
2006	21	317	**338**
2005	46	339	**385**
2004	24	190	**214**
2003	27	189	**216**
2002	14	189	**203**
2001	20	54	**74**
2000	2	113	**115**

Lähde: Polstat 3.9.2012

6.9.2012

Haaste yhteiskuntatieteelliselle tutkimukselle

- Yhteiskunnallinen ilmiö, joka koskettaa kansalaisia, yrityksiä ja viranomaisia
- Teknisyys karkottaa kiinnostuneet?

- Uhrikyselyt kansalaisille
- Uhrikyselyt/haastattelut yrityksille
- Kyselyt/haastattelut rikollisfoorumeilla
- Rekisteriaineistot: vain vähän oikeustapauksia, poliisille ei ilmoiteta, CERT-FI

Tuoreempia lähestymisvaihtoehtoja

- Online keskustelut: esim. keskustelufoorumit, IRC-kanavat ym.
- Muut digitaaliset jäljet? Automaattinen monitorointi

- Eri alojen tutkijoiden keskinäinen yhteistyö
- Yhteistyö myös kaupallisten tietoturvayhtiöiden ja ohjelmistovalmistajien ym. kanssa -> heillä on usein ajantasaisin tieto verrattuna akateemisiin

Tietoverkkorikostutkinnan toimintaympäristö, organisointi ja viranomaisyhteistyö -tutkimus

- Toteutus 2013 – 2016 artikkeliväitöskirjana
- Tampereen yliopisto, turvallisuushallinto (Turvallisuuden tutkimusryhmä) & Poliisiammattikorkeakoulu
- Tavoitteet:
  - luoda kuva Suomeen kohdistuvasta tietoverkkorikollisuudesta sekä kehittää uusia tapoja syventää viranomaisten tilannekuvaa tietoverkkorikollisuudesta
  - selvittää kuinka poliisin tietoverkkorikostutkinnassa voidaan tehdä aiempaa vaikuttavampaa yhteistyötä eri viranomaisten ja yksityisten toimijoiden kanssa

6.9.2012

Kiitos!

Lisätietoja:
Anna Leppänen
p. 050 399 7679
anna-riitta.leppanen@poliisi.fi

6.9.2012

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

SIEM ja Kybertilannekuva

Vesa Keinänen, Senior Network Security Specialist, CISSP, Insta DefSec

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

SIEM ja Kybertilannekuva

Vesa Keinänen

Senior Network Security Specialist, CISSP

Insta DefSec

Insta Group ja Insta DefSec Oy

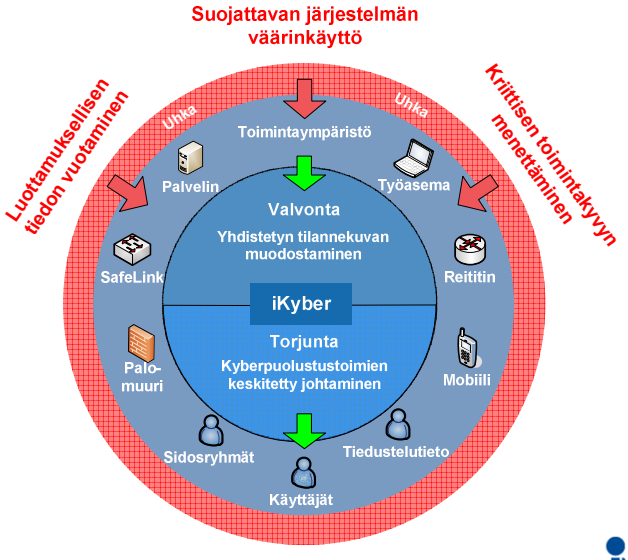
Insta Group

- Insta Group Oy on perheyritys, jonka juuret ulottuvat vuoteen 1960. Nykyään meillä työskentelee jo noin 700 osaajaa innovatiivisten tuotteiden, ratkaisujen ja palvelujen parissa
- Vahvan kasvun ja kansainvälistymisen aikaa elävä yritys on erikoistunut kahteen toimialaan, jotka ovat:
  - puolustus- ja turvallisuusteknologia (Insta DefSec Oy)
  - teollisuusautomaatioteknologia (Insta Automation Oy).

Insta DefSec Oy

- Insta DefSecin yli 300 henkilöstä noin 250 työskentelee tehtävissä, jotka liittyvät turvallisuusviranomaisten järjestelmien, vahvan tietoturvan sekä palvelutuotannon tarjoamiseen.

iKyber-järjestelmä



Terminologiaa

ISO 27002

Information Security Event, tietoturvatapahtuma

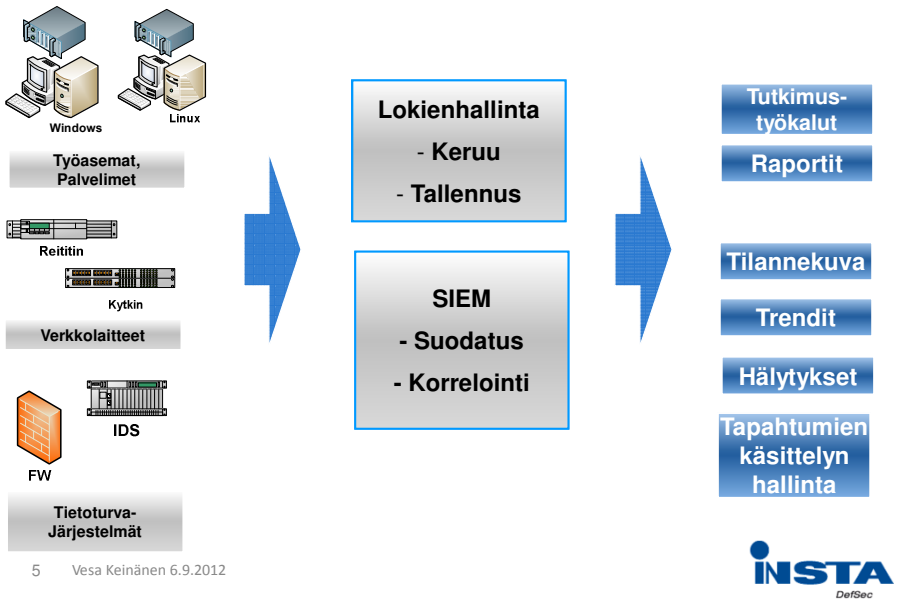
- an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information Security incident, tietoturvapoikkeama

- an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

SIEM-järjestelmässä käsitellään mitä tahansa informaatiota, jolla voi olla merkitystä tietoturvan tilan seurantaan tai tietoturvapoikkeamien tunnistamiseen.

SIEM, Security Information and Event Management



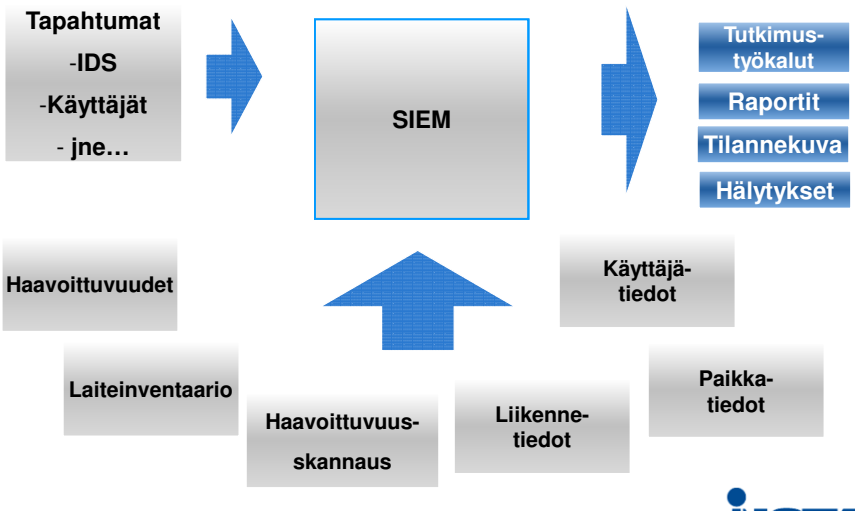
5 Vesa Keinänen 6.9.2012

Lokien hallinta ja SIEM

Lokien hallinta	SIEM Security Information and Event Management
▪ **Lokien keruu eri järjestelmistä**	▪ **Kerätyn lokitiedon analysointi**
▪ Tapahtumien yhtenäistäminen (normalisointi) ▪ Tapahtumien luokittelu ▪ Lokien tallennus ▪ Tapahtumien selailu- ja tutkimistyökalut ▪ Raportointi ▪ Yksinkertaiset hälytykset	▪ Korrelointi ▪ Erillisten tapahtumien yhteenlinkitys ▪ Trendianalyysi ▪ Anomaliatunnistus ▪ Hälytykset ▪ Raportointi
▪ Analysointiominaisuudet (raportointi) nojautuu tallennetun datan käsittelyyn jälkikäteen	▪ Lähes reaaliaikainen ja historiallinen analysointi

6 Vesa Keinänen 6.9.2012

Tietojen yhdistäminen



7 Vesa Keinänen 6.9.2012

SIEM-järjestelmän tekniset komponentit

Tapahtumien keruu, normalisointi ja luokittelu

- Lokitietojen / tapahtumien muuntaminen yhtenäiseen muotoon
- Mahdollistaa lähderiippumattoman datan jatkokäsittelyn ja analysoinnin
- Lokienhallinta- ja SIEM-järjestelmät sisältävät tuen tavallisimmille lokilähteille
- Erityiset lähteet vaativat räätälöintiä

Korrelointi

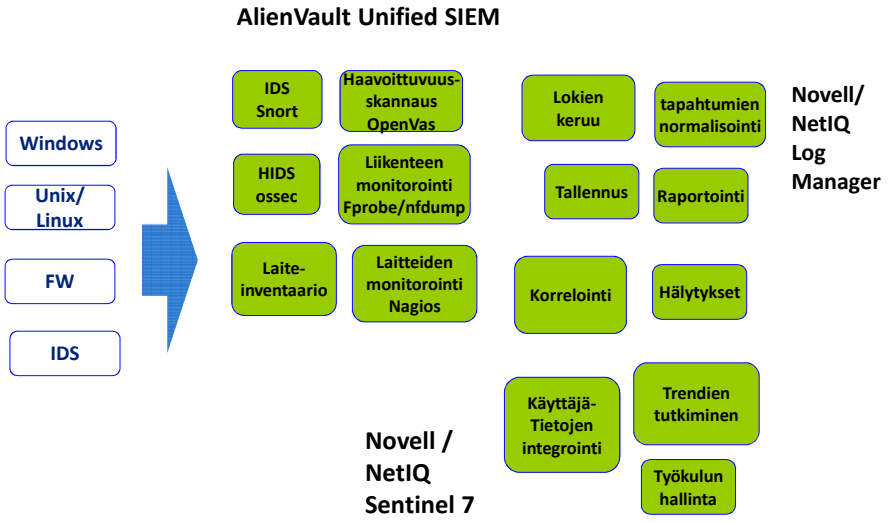
- Sääntöpohjainen tapahtumasarjojen tunnistaminen
  - Hyökkäysten ja epätyypillisten tilanteiden automaattinen tunnistus
- SIEM-järjestelmä sisältää mallisääntöjä, vaatii räätälöintiä paikalliseen ympäristöön
- Sääntöjen ylläpito jatkuvaa toimintaa

Trendien analysointi

- Valittujen tapahtumien määrän seuranta
- Epätavallisten tilanteiden automaattinen tunnistus (anomaliatunnistus)

8 Vesa Keinänen 6.9.2012

Tutkitut SIEM-järjestelmät



SIEM-käyttöönotto

Toteutusmalli
- **Tietoturvapäällikkö asettaa tavoitteet**
- **Tietoturva-asiantuntija hoitaa toteutuksen**

Aloita tästä!

Aseta tavoitteet:
- Mitä kerätään
- Mitä tutkitaan
- Mitä raportteja / hälytyksiä / trendejä halutaan nähdä

Konfiguroi lokien keruu eri lokilähteistä

Konfiguroi/räätälöi raportteja

Konfiguroi hälytykset

Konfiguroi lokien normalisointi

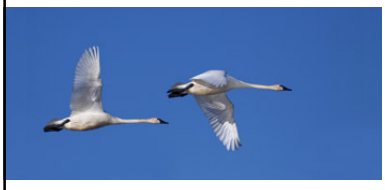
-valmiit säännöt
- räätälöinti

Konfiguroi analysointi/korrelointi

Kysymyksiä?

INSTA DefSec

Kiitos!



Yhteystiedot

Insta DefSec
Vesa Keinänen
Senior Network Security Specialist, CISSP

Sarankulmankatu 20
FIN-33901
Tampere

Tel: 050 – 3592433
Email: vesa.keinanen@insta.fi

www.security.insta.fi

INSTA DefSec

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Reliability of the Internet IXP Role

Aleksi Suhonen, BaseN / Trex.fi

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

TREX
TAMPERE REGION EXCHANGE

Reliability of the Internet
IXP Role

Aleksi Suhonen

2006/05/17

TREX
TAMPERE REGION EXCHANGE

TREX
TAMPERE REGION EXCHANGE

First some jargon:

IXP Internet Exchange Point.

ISP Internet (or Network) Service Provider.
aka network operators

peering Agreement to exchange own and customers' traffic.

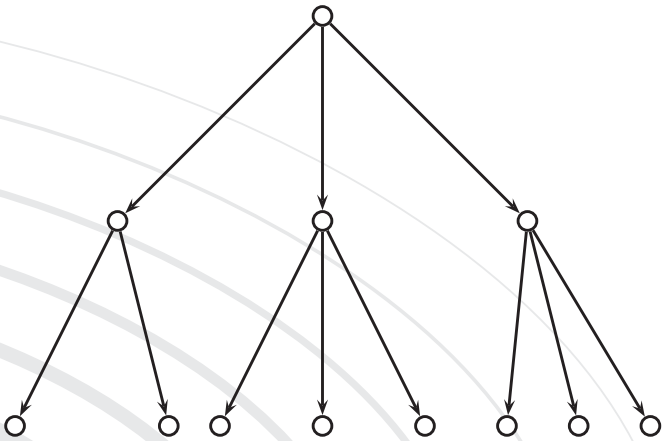
transit Agreement to carry all traffic.

TREX
TAMPERE REGION EXCHANGE

Basics and Background

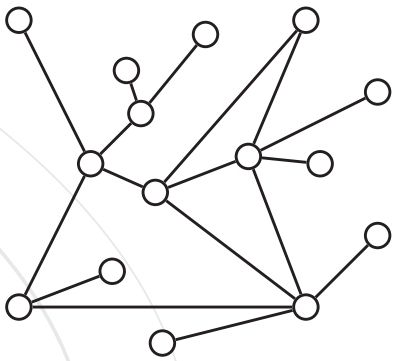
The Internet is a network of interconnected networks. There is no overall structure to the network.

Compare the Telephone Network...



Hierarchical Network

Network of Networks



...with the Internet.

Initially networks were interconnected only via private lines.

As the number of networks grew larger, the number of private lines grew very fast. ("$O(n^2)$")

Two concepts attenuated this growth: transit and exchanges.

TREX
TAMPERE REGION EXCHANGE

Internet Exchanges

It is cheaper for all ISPs to connect to one location (i.e. IXP) to meet other ISPs instead of every ISP connecting directly to every other ISP.

According to different estimates 50 – 90 percent of European Internet traffic flows over IXPs.

In Northern America IXPs carry only 10 – 50 percent of all traffic. Private peering is more popular in the US.

TREX
TAMPERE REGION EXCHANGE

Traffic Growth

There have been several paradigm shifts in what most of the traffic on the Internet is about during its brief history. Here's some examples:

- bulk traffic (mail, news) → surfing (ftp, http)
- surfing → download and consume (music)
- download and consume → streaming (video)

TREX
TAMPERE REGION EXCHANGE

Traffic Growth (continued)

- New usage patterns emerge that will drown out old ones.
- Network usage caused by old patterns does not dimish!
- Consumer usage has surpassed research and business usage.
- Domestic network usage will still continue to grow.
- New user classes will continue to emerge. (e.g. m2m)
- Tendency toward applications that require more and more reliability.

TREX
TAMPERE REGION EXCHANGE

TREX
TAMPERE REGION EXCHANGE

Neutrality

ISPs don't easily place trust in an IXP that is essentially a product of a rival ISP.

⟶ IXPs need to try to stay neutral.

Neutrality plays a role in many other aspects too.

©2006 Aleksi Suhonen

TREX
TAMPERE REGION EXCHANGE

Redundancy and Capacity

ISPs usually connect to most exchanges located in the area where the ISPs operate.

- keeps traffic local
- each IXP adds to the total bandwidth available between ISPs
- traffic shifts to close by IXPs in case of any failures
  (as opposed to transits or trans-oceanic IXPs)

TREX
TAMPERE REGION EXCHANGE

Services

- clock synchronization source
- root name servers
- ...

TREX
TAMPERE REGION EXCHANGE

Forum

for...

- debugging problems
- sharing experiences
- spreading information

...affecting the wider network

TREX
TAMPERE REGION EXCHANGE

Forum can be:

- mailing list
- workshop
- seminar or conference

Some IXPs also take part in societal discussion.

End of Slides

- Open discussion
- Q and A?
- `http://iplu.vtt.fi/`
- `http://www.trex.fi/`

kyberturvallisuus
hyökkäys ja
puolustus
seminaari 6.9.2012

Läpinäkyvä käyttäjähallinta ja salaus kyberavaruudessa

Mikko Jakonen, Security / technology specialist, Mikko Jakonen Ltd.

CIRCMI

6. syyskuuta 2012

Tampereen yliopisto

P/I/T/K/Y

~Läpinäkyvä käyttäjähallinta ja salaus kyberulottuvuudessa~

Mikko Jakonen: Ubiquitous model for managing role based identities and encryption capabilities within cyberspace (including clouds) –tutkielma 11/2012

KYBERTURVALLISUUS 6.9.2012

mikko@jakonen.net

Eli ”Konsepti X”

.me

Määrittelyt on tänään jo annettu ☺

Kyberavaruus = **Internet** = **Cloud** tai mikä tahansa muu **ympäristö** jossa informaatiovirtoja voidaan käsitellä, hyödyntää ja hallita tietoteknisin keinoin.

Tämä EI ota kantaa onko käytettävä tietotekninen ympäristö valtiollinen, kaupallinen tai yksityinen

Lyhyesti

Pureudutaan haasteeseen jota ei ole vielä mietitty (riittävästi) ja josta *voi* olla merkittävästi hyötyä tulevaisuudessa ja jota eri kyber- ja palvelutoimijat kaipaavat jo nyt.

Huom! Tämä EI ratkaise kaikkia haasteita joita tunnistamme.

Esityksen #TECHNICAL_LEVEL ~2, BS_LEVEL ~1

Muutos ☺

Eli mihin Konsepti X:n pitäisi kyberturvallisuudessa **muunmuasssa** vastata osaltaan, kun maailma muuttuu alla...

Tausta-ajatuksia ...”strategems” w/Konsepti X @ Cyberspace

”Pakottaa kohdennetusta tiedustelusta laajakaistaista”

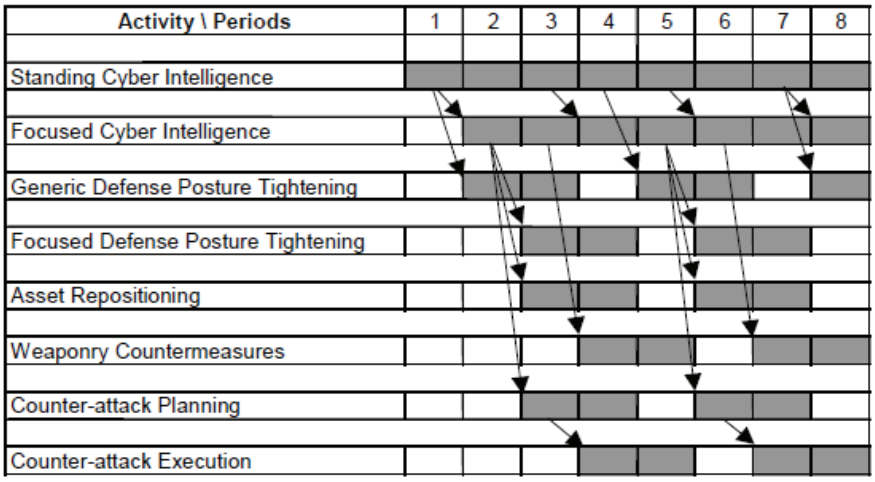
”Parantaa turvallisuuden olotilaa”++

”Vähentää riippuvuutta”

”Ymmärtää mitä on käsissä”

”Nopeuttaa puolustusta”

”Integroida itsestäänselvyydet”



...taktiikoissa...

- **Tiedolle** voidaan asettaa taktinen ”aika”; ja syödä sitä loppupäästä ~ asettaa vanha tieto käyttökelvottomaksi. **Elinkaarihallinta**.
- Laajojen, epäsymmetristen käyttäjäjoukkojen valtuushallinta saadaan valtavan **nopeaksi**.
- ...ja ennenkaikkea **läpinäkyvä**ksi.
- **Linnoittaa** käyttövaltuushallinnan pilveen vs. tehdä sitä yksittäisten toimijoiden kanssa.
- **Iskunkestävyys.** Hajauta ja hallitse ☺

...toiminnoissa ja operatiivisesti

- Tavoitteena 100% läpinäkyvyys käyttäjälle ja ymmärrys ”ymmärryksestä” omalla vektorillaan.
- Lamauttamisen vaikutus heikkenee ja sen tuottaminen vaikeutuu.
- ”Attribution”; sivuvaikutusten mitigointi.
- Jos mitään ei ole tehty → oman kyvykkyyden kasvattaminen.
- ”Tiedonhallinnan resilienssi” kasvaa; ymmärrys henkilöiden suhteesta tietoon ja sen käyttöön.

MAHDOLLISTAA oikea informaatioresurssien käyttö TURVALLISESTI

Eli EI torju sovellusheikkouksia, eikä ihmisten laiskuutta. Eikä rakenna uusia verkkoja, ei tuo uusia purkkeja nurkkiin eikä muuta ”pelin” sääntöjä itsessään.

MUTTA...

→ In practical terms

Konsepti X - ”ulkona cybersodasta”

Miksi otsikko on noin piiiitkä?

- ***Ubiquitous** model for managing **role based identities** and **encryption** capabilities within **cyberspace** (including clouds)*

= Kyberavaruus on iiissooooooo!

Ei ole mahdollista sanoa tätä lyhyemmin, vielä.

Käyttäjähallinta ja salaus *lyhyt, lyhyt* –historia. Yhdessä.

#1

”&h327dyt#”!”

Valmistajakohtainen
Sovelluskohtainen

#2

”&h327dyt#”!”

My iEverything

Kestämätön tilanne
Ratkaisut erilaisia

#3

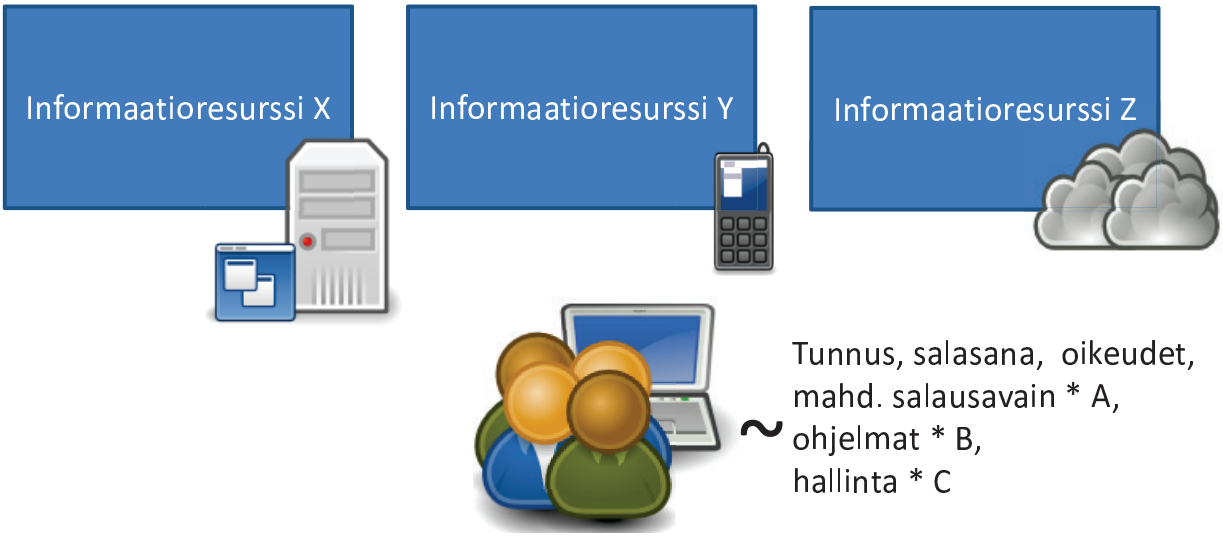
My secretdata.txt

Soveltuvia salausratkaisuja huonosti tarjolla

Näitä ei ole tähän mennessä nähty koskaan linkitettynä toisiinsa...outoa?

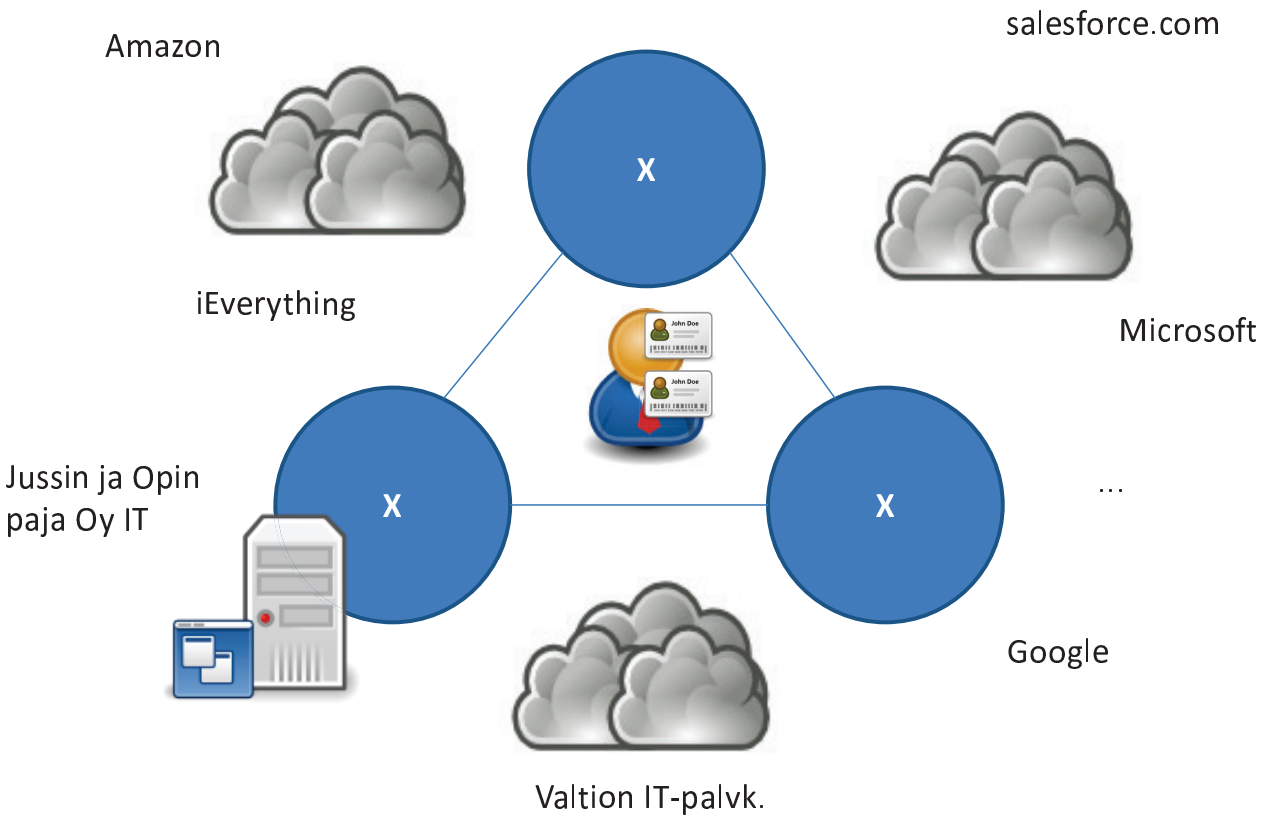
Tilannekatsaus ”IdM in a cloud” + crypto

- 
- Pilvipalvelu vs. inhouse/on-premises = samat ongelmat. Ei salata.



Haasteita

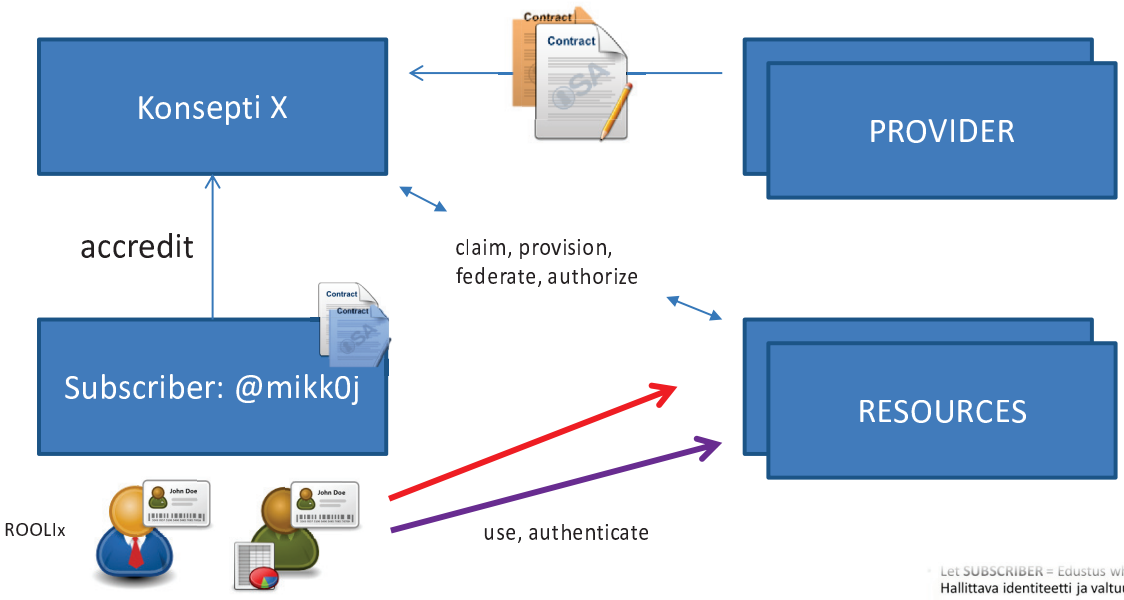
- Käyttövaltuuksia myönnetään irrallaan toisistaan eri tahojen toimesta
  - Ei se mitään, se on ihan ok!
  - Sisäinen/ulkoinen kyberavaruus, valtuuksien elinkaaren hallintaja useat toimijat/toimijaketjut...tekee hommasta raskasta.
- Salausta harjoitetaan, jos harjoitetaan (eli ei).
  - Fine, jos näin on sovittu. Tokihan tiedämme mikä tieto on arvokasta...
  - Silti olemme huolissamme mitä arvokasta tietopääomaa valuu → 
  - Luodaan ”toissijaisia ratkaisuja”



Konsepti X

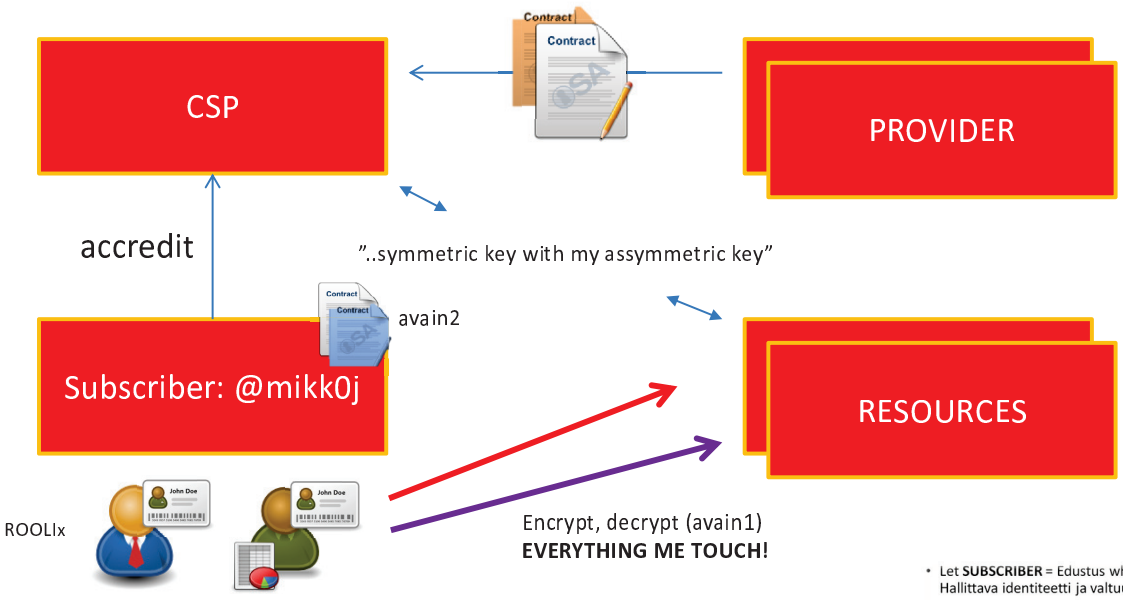
- Let **SUBSCRIBER** = Edustus where **ROOLI**x = Hallittava identiteetti ja valtuus
- Let **CONTRACT**x = Palvelusopimus
- Let (**s**)**PROVIDER**x = ”IT PALVELUKESKUS”
- Let **RESOURCE**x= Informaatioresurssi; on-premises tai cloud.
- Let **AVAINx** = ROOLIn salausavain, Let **AVAIN2** = SUBSCRIBERin salausavain
- **Konsepti X** applikaatio = Jonkinlainen CSP ”Cloud Security Platform”; tarjoaa IdM/IdP sekä tietyt cryptopalvelut.

...eli käyttövaltuuksien hallinnassa?



- Let **SUBSCRIBER** = Edustus where **ROOLI** = Hallittava identiteetti ja valtuus
- Let **CONTRACT** = Palvelusopimus
- Let (s)**PROVIDER** = "IT PALVELUKESKUS"
- Let **RESOURCES** = Informaatioresurssit; on-premises tai cloud.
- Let **AVAIN ^1** = ROOLIn salausavain, Let **AVAIN^2** = SUBSCRIBERin salausavain
- Let **CSP** = **Konsepti X** applikaatio.

...eli salauksen hallinnassa?



- Let **SUBSCRIBER** = Edustus where **ROOLI** = Hallittava identiteetti ja valtuus
- Let **CONTRACT** = Palvelusopimus
- Let (s)**PROVIDER** = "IT PALVELUKESKUS"
- Let **RESOURCES** = Informaatioresurssit; on-premises tai cloud.
- Let **AVAIN ^1** = ROOLIn salausavain, Let **AVAIN^2** = SUBSCRIBERin salausavain
- Let **CSP** = **Konsepti X** applikaatio.

Hierakiasta - אין בעיות

- mm.

Sopimus

- Sopimus on päätös toimijoiden välisestä valtuushallinnasta. Yksi tai useampia.
- Kun sopimus revoikoidaan, oikeudet poistuvat

Salaus

- Kun oikeudet poistuvat, siirtyy avain esim. providerille (sopimuksen mukaan).
- Kun salausavain poistetaan, pääsy tietoihin estyy.
- Salaus toimii vain yhdessä roolien kanssa
- Salataan vain dataa ”in-rest”. Datan sijainnilla ei merkitystä.

Valtuushallinta

- Hallittava moniedustuksellisuus ☺ - ts, ”sinulla on JO tili iCloudissa.
- Ymmärrys henkilöiden ja organisaatioiden suhteista.